Analisis DFXML Untuk Mendukung Identifikasi dan Pengelolaan Artefak Digital Pada Aplikasi TikTok

Muhammad Romi Nasution
18917122

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2022

Lembar Pengesahan Pembimbing

Analisis DFXML Untuk Mendukung Identifikasi dan Pengelolaan Artefak Digital Pada Aplikasi TikTok

Muhammad Romi Nasution
18917122

Yogyakarta, Mei 2022

Pembimbing I	Pembimbing II
Dr. Yudi Prayudi, S.Si., M.Kom.	Ahmad Luthfi, S.Kom., M.Kom., Ph.D.

Lembar Pengesahan Penguji

Analisis DFXML Untuk Mendukung Identifikasi dan Pengelolaan Artefak Digital Pada Aplikasi TikTok

Muhammad Romi Nasution

18917122

Yogyakarta, Mei 2022

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom.
Ketua

Ahmad Luthfi, S.Kom., M.Kom., Ph.D.
Anggota I

Dr. Ir. Bambang Sugiantoro, S.Si., M.T.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Iriving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Analisis DFXML Untuk Mendukung Identifikasi dan Pengelolaan Artefak Digital Pada Aplikasi TikTok

Penelitian ini melakukan pengembangan identifikasi dan menganalisis artefak digital aplikasi TikTok. Serta, memetakan karakteristik bukti digital yang relevan jika terdapat lebih dari satu akun. Pengembangan juga dilakukan pada fungsional agar lebih lengkap dalam visualisasi identifikasi pada aplikasi Autopsy. Pengujian terhadap berkas XML sekitar 100 lebih item. Namun, tidak semua item di dapat informasi dari kegiatan pelaku. Berkas yang terpenuhi dari tiga akun adalah aweme_user.xml. Setiap akun akan tersimpan kegiatannya pada berkas tersebut walaupun akun telah dihapus di dalam sistem aplikasi TikTok. Konteks penelitian ini dibagi menjadi 3 bagian diantaranya sangat dibutuhkan, kurang dibutuhkan dan tidak dibutuhkan. Pada bagian sangat dibutuhkan seperti berkas aweme_user, version, search dan lain-lain. Adapun kurang dibutuhkan tetap akan dianalisis untuk mendukung isi data XML dari berkas kategori sangat dibutuhkan. Semua gambar memiliki jumlah sekitar 200 item lebih, karakter dari gambar secara garis besar ada 4 bagian pertama Nama seperti img_7216, img_7217 dan seterusnya, selain itu menggunakan format tahun bulan dan tanggal kemudian akhiran nama "cover" pada sebagian gambar seperti, gambar-gambar yang ada yaitu hasil dari belhan video menjadi gambar dan ekstensi dalam kompres potongan gambar menggunakan png. Berkas XML yang cukup lengkap informasinya dari 3 akun adalah awemeuser.xml seperti tempat pencatatan alamat masuk, username, metode masuk, terakhir diakses dan lain-lain. Dapat disimpulkan informasi terbanyak ada pada berkas tersebut. Hasil analisis informasi terbanyak terdapat pada aweme_local_video.xml dan LoginSharePreferences.xml. aweme_local_video.xml adalah tempat penyimpanan jejak kegiatan unggah video. Jadi letak direktori dari berkas video dapat dilihat pada file XML tersebut. LoginSharePreferences.xml adalah informasi login akun yang telah dihapus.

Kata kunci

Artefak Digital, TikTok, DFXML, File System XML

Abstract

DFXML Analysis to Support the Identification and Management of Digital Artifacts in the TikTok App

This study develops identification and analysis of digital artifacts for the TikTok application. Also, map the characteristics of relevant digital evidence if there is more than one account. Development is also carried out on the functional so that it is more complete in the identification visualization in the Autopsy application. Testing against an XML file of about 100+ items. However, not all items can be obtained from the activities of the perpetrators. The satisfied file of the three accounts is aweme_user.xml. Each account will have its activities stored in the file even if the account has been deleted in the TikTok application system. The context of this research is divided into 3 parts which are very much needed, less needed and not needed. In the much needed sections such as aweme_user file, version, search and others. The less needed will still be analyzed to support the XML data content of the badly needed category file. All images have more than 200 items, the character of the image in general there are 4 first parts Names such as img_7216, img_7217 and so on, in addition to using the year, month and date format then the name suffix "cover" on some images such as, there is the result of converting video into images and extensions in compressing image pieces using png. A fairly complete XML file with information from 3 accounts is awemeuser.xml such as a place to record login addresses, usernames, login methods, last accessed and others. It can be concluded that the most information is in the file. The results of the analysis of the most information are found in aweme_local_video.xml and LoginSharePreferences.xml. aweme_local_video.xml is where video upload traces are stored. So the directory location of the video file can be seen in the XML file. LoginSharePreferences.xml is the login information of the account that has been deleted.

Keywords

Digital Artifact, TikTok, DFXML, File System XML

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Mei 2022

Muhammad Romi Nasution, S. Kom.

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dari Bab 3

Kontributor	Jenis Kontribusi
Muhammad Romi Nasution	Mendesain eksperimen (70%) Menulis *paper* (75%)
Yudi Prayudi	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)
Ahmad Luthfi	Mendesain eksperimen (10%) Menulis dan mengedit *paper* (10%)

Halaman Kontribusi

Penelitian ini tidak terlepas dari berbagai saran maupun bimbingan dan berbagai pihak, mulai dari penelitian, seminar proposal, seminar progress, hingga seminar pendadaran. Pihak-pihak tersebut, antara lain, Dr. Yudi Prayudi, S.Si., M.Kom dan Ahmad Luthfi, S.Kom., M.Kom., Ph.D.

Halaman Persembahan

Bismillahirrahmanirrahim.

Alhamdulillah atas ridho Allah Subhanahu Wa Ta'ala karya ini saya persembahkan kepada kedua orang tua dan kawan-kawan yang telah mendukung, memberikan semangat dan motivasi dalam menyelesaikan pendidikan magister komputer saya ini, secara khususnya kepada:

1. Ayahanda (Paisar NST) dan Ibunda (Delinar HSB) yang selalu mendo'akan anaknya menjadi orang yang berguna seperti yang diharapkan, baik bangsa, dan tentunya agama. Dan yang terpenting adalah pengorbanan yang tak lekang oleh masa dan tak terbalas oleh upaya.
2. Abang (M Taufik NST) dan Kakak (Siti Aminah LBS) yang selalu mendukung baik dari segi moril maupun materil. Dan yang terpenting adalah saling mengingatkan dan menjaga dalam kekompakkan.
3. Istri tercinta (Melkiana HSB) dan anak (M Elea N) yang menjadi penyemangat dalam dunia pendidikan dan tentunya masa depan. InsyaAllah, yang terpenting adalah ibu yang salihah buat anak-anak saya yang salih-salihah (Aamiin).
4. Tidak lupa tentunya kepada kawan-kawan seperjuangan Forensika Digital '18 yang memberikan dukungan selama menempuh pendidikan ini.

Kata Pengantar

Assalamu'alaikum Warohmatullahi Wabarokatuh.

Puji syukur penulis haturkan kepada Allah SWT atas limpahan rahmat dan karunia yang diberikan kepada penulis sehingga dapat menyelesaikan laporan penelitian tesis yang berjudul "*InterPlanetary File System* pada *Digital Evidence Cabinet* berbasis *Hyperledger Fabric* untuk Manajemen Bukti Digital". Adapun maksud dari penulisan laporan penelitian ini adalah sebagai persyaratan dalam mencapai jenjang pendidikan Magister Informatika konsentrasi Forensika Digital di Fakultas Teknologi Industri, Universitas Islam Indonesia. Dalam proses penyelesaian tesis ini penulis tidak dapat menyelesaikannya bila tidak ada turut serta pihak lain yang juga ikut membantu baik secara langsung maupun tidak langsung. Untuk itu penulis ingin menyampaikan rasa terima kasih kepada beberapa pihak yang telah mendukung dalam penyusunan tesis ini, antara lain:

1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D, selaku rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk menimbah ilmu di Universitas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D, selaku Ketua Program Studi InformatikaProgram Magister Fakultas Teknologi Industri, Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr. Yudi Prayudi, S.SI., M.Kom, dan Bapak Ahmad Luthfi, S.Kom., M.Kom., Ph.D. selaku dosen pembimbing yang telah banyak meluangkan waktunya dalam memberikan berbagai saran selama proses bimbingan.
5. Seluruh Dosen, staff administrasi dan civitas Magister Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama masa studi penulis.
6. Seluruh keluarga baik Bapak, Ibu, Abang, dan Kakak yang telah mencurahkan segenap cinta, kasih sayang, perhatian dan dukungan baik moril maupun materil.
7. Rekan-rekan mahasiswa MI khususnya konsentrasi Forensika Digital angkatan 18 yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain. dalam penyusunan laporan tesis.

Adapun yang masih ada kekurangan maupun kesalahan dalam laporan ini, penulis membuka lebar kritik dan sarannya agar dapat diperbaiki supaya kedepannya lebih maksimal sesuai yang diinginkan. Akhir kata dari penulis, terimakasih sebesar-besarnya semoga laporan ini bermanfaat dan bisa membantu rekan-rekan yang membutuhkan khususnya mahasiswa/mahasiswi Universitas Islam Indonesia.

Wassalamu'alaikum Warahmatullahi Wabarokatuh.

Daftar Isi

Daftar Tabel

Daftar Gambar

BAB 1
Pendahuluan

1.1 Latar Belakang

Keunggulan TikTok dalam menyajikan konten video pendek begitu kreatif dan menarik. Sebagian penggunanya membuat konten untuk mendapatkan lebih banyak perhatian dan pengakuan sehingga meningkatkan sosialitasnya. Setiap konten yang diunggah sepenuhnya dapat dieksplorasi jika sudah saling mengikuti, sepanjang kontennya memiliki keunikan yang menghibur orang lain, umpan balik secara *realtime* pasti ada dari penontonnya (Wang et al., 2019).

Konten aplikasi TikTok memiliki sisi gelap. Seperti aliran peredaran obat-obatan, penyiksaan dan membunuh binatang, kata-kata kotor, melecehkan satu sama lain, pornografi, predator anak-anak, ekstremisme dan pelecehan suatu agama. Tahun 2019, Politisi India menyarankan agar TikTok dilarang karena konten seksual eksplisit, *cyber bullying* dan *deepfake.* Konten Ekstremisme pada Oktober 2019, dilaporkan ada perekrutan anggota ISIS. Video tersebut menggunakan filter hati dan musik *catchy,* kontennya menampilkan seorang pria memegang senjata dan satu orang pria memenggal kepala seseorang. Diikuti dengan suara tembakan serta lagu ISIS yang mengagungkan militer mereka, tampaknya konten tersebut menargetkan anak muda dengan menggunakan istilah "*Jihad Lover*" dan "*Jihadist* and *Proud*"[1].

Hasil investigasi *British Sun Online* (Media) mengungkapkan, bahwa ada unggahan yang mengandung ekspos anak-anak dan remaja[2]. Konten ujaran kebencian ditemukan oleh SPLC (*Southern Poverty Law Center*) pada Desember 2019, unggahan tentang supremasi kulit putih secara kejam, tentang nazisme serta seruan untuk membunuh Yahudi dan Kulit Hitam dengan kata-kata "*kill all nigga*", "*all jews must die*" dan "*killnigga*" pada unggahan[3].

Tahun 2018, TikTok pernah dilarang untuk beroperasi di Indonesia karena mengizinkan penyebaran konten pornografi dan pelecehan agama. Namun, pada pertengahan tahun 2020 terdapat kasus seorang remaja mengunggah video shalat sambil berjoget. Judulnya "Pas lagi solat, tiba² ada tetangga puter lagu DJ, dari pada gak khusyuk,

---

[1] https://www.cnbc.com/2019/10/21/tiktok-removes-two-dozen-accountsused-for-isis-propaganda.html

[2] https://www.thesun.co.uk/news/10962862/tiktok-extremist-racist-videos-anti-semitism/

[3] https://www.vice.com/en/article/yw74gy/tiktok-neo-nazis-white-supremacy

iaaaa keburu suami datang". Wanita tersebut, dikenai Pasal 156 KUHP dan Undang - Undang ITE dengan ancaman hukuman 5 tahun penjara[4]. Pada Oktober 2020 pelecehan agama dilakukan oleh @kenwilboy, setelah diinterogasi alasan pelaku konten tersebut dibuat hanya untuk menambah *follower*. Tersangka diancam dengan hukuman 6 tahun penjara dijerat dengan Undang-undang ITE[5]. Kasus tindakan kriminal menggunakan aplikasi TikTok begitu banyak. Sementara itu, penelitian tentang identifikasi artefak digital dari aplikasi TikTok masih terbagi dalam parameter yang berbeda-beda akan tetapi memiliki tujuan yang sama.

Menurut penelitian (Hoang Khoa et al., 2020) File XML dapat diidentifikasi dengan Tiga parameter. Diantaranya teman, pengguna dan pencarian. File XML pada dasarnya memberikan Tujuh informasi. Yakni waktu aplikasi dibuka, dipasang, diperbaharui, MAC address, pencarian, bahasa dan region.

Penelitian berikutnya oleh (Domingues et al., 2020) menggunakan metode Post-Mortem dalam mengidentifikasi artefak pada TikTok. Hasilnya, menemukan Tiga *file* XML penting yakni pengguna, Cara masuk dan pencarian. Penelitian tersebut juga menggunakan sebuah modul Autopsy yang dapat mengidentifikasi fungsional teman dan pesan.

Penelitian ini menggunakan DFXML dan membuat peta singkat untuk menemukan artefak-artefak penting dari sekian banyaknya berkas yang ditinggalkan dipenyimpanan ponsel. Diketahui, pada aplikasi TikTok terdapat lebih dari dua fungsional. Seperti, unggah video, suka, komentar dll. Penelitian ini melakukan pengembangan identifikasi dan menganalisis artefak digital aplikasi TikTok. Serta, memetakan karakteristik bukti digital yang relevan jika terdapat lebih dari satu akun. Pengembangan juga dilakukan pada fungsional agar lebih lengkap dalam visualisasi identifikasi pada aplikasi Autopsy.

[4] https://www.liputan6.com/news/read/4246441/polisi-jerat-perempuan-salat-sambil-joget-tik-tok-dengan-pasal-penistaan-agama

[5] https://www.kompas.tv/article/113699/pelaku-tiktok-pelecehan-masjid-meminta-maaf-kepada-masyarakat

1.2 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah:

1. Bagaimana melakukan analisis berkas XML aplikasi TikTok di Android untuk memetakan karakteristik bukti digital yang relevan jika terdapat lebih dari satu akun?
2. Bagaimana memetakan berkas XML yang diperlukan untuk investigasi pada aplikasi TikTok?

1.3 Batasan Masalah

Batasan masalah penelitian ini sebagai berikut:

1. Pengujian terhadap aplikasi media sosial TikTok versi 16.6.4.
2. Melakukan pengujian pada Xiaomi Redmi 5 Android versi 10.0
3. Menganalisis 3 akun TikTok
4. Menambahkan fungsional modul Android *analyzer* diantaranya *Searching*, *Followers*, *Favorite*, *Information User*, *Video*

1.4 Tujuan Penelitian

Ada beberapa tujuan pada penelitian media sosial TikTok ini diantaranya:

1. Melakukan penelitian mengenali karakteristik bukti digital pada media sosial TikTok
2. Melakukan pemetaan berkas pada aplikasi TikTok.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat yang dapat digunakan oleh penyidik dalam menganalisa bukti digital pada aplikasi TikTok. Diantara manfaatnya adalah:

1. Memberikan solusi adanya cara untuk membaca karakteristik artefak digital dari telepon pintar yang menggunakan OS Android jika lebih dari satu akun.
2. Mengetahui cara pengambilan berkas penting untuk keperluan identifikasi.

1.6 Review Penelitian

Penelitian oleh (Anglano, 2014) analisis *database* pada kontak untuk merekonstruksi daftar kontak di aplikasi WhatsApp *Messenger.* Hasilnya penyelidik dapat menemukan ketika kontak telah ditambahkan, memulihkan kontak yang dihapus dan menemukan waktu penghapusannya. korelasi dengan pesan yang dikirim penyidik dapat mengidentifikasi pesan yang telah dihapus dan kapan pesan tersebut dikirim. Penelitian ini menggunakan Emulator

Android YouWave yang menjalankan Android versi 4.4.4 sebagai lingkungan analisisnya. Penelitian pada emulator ada yang tidak dapat di ekstraksi yaitu posisi (GPS). Sebab, tidak memungkinkan karena emulator yang digunakan tidak mendukung. Sehingga *region* di *file log* tidak tersedia.

Penelitian (Ali & Fazeel, 2016), identifikasi artefak digital pada aplikasi *Facebook*, *Twitter* dan *LinkedIn* di sistem operasi Android, iOS, Windows dan BlackBerry. Cara yang digunakan adalah ekstrak *disk image* selanjutnya melakukan analisis pada berkas *database*. Semua aplikasi yang diuji memiliki karakteristik yang berbeda setiap sistem operasi, tantangannya semakin hari akan semakin banyak media sosial yang perlu di analisis.

Peneliti (Anglano et al., 2017), dapat mengidentifikasi semua artefak Telegram *Messenger* di Android. Secara khusus, peneliti telah membahas metode untuk menafsirkan data yang disimpan dalam *database* dan *file* konfigurasi pengguna. Hasilnya dapat merekonstruksi daftar kontak, pesan tekstual dan non-tekstual yang dipertukarkan serta menentukan apakah pengguna membuat atau mengelola obrolan rahasia, grup dan saluran.

Selanjutnya penelitian (Cedillo et al., 2019) melakukan penelitian tentang *Log Activity*. Hasilnya, dapat melihat aktivitas yang dibagi menjadi 5 jenis: riwayat penelusuran web, *cookie*, gambar, unduhan, dan *instan messenger.* Adapun riwayat penjelajahan, 11 halaman web ditemukan. Sedangkan untuk *cookie* ada 8 aktivitas, kemudian 4 gambar yang dapat dipulihkan. *File* PDF ditemukan dalam aktivitas unduhan dan pesan audio pada aplikasi WhatsApp.

Metode penelitian (Hoang Khoa et al., 2020) adalah dengan menganalisis artefak yang tertinggal di telepon pintar Android. Hasilnya, menjawab pertanyaan secara umum diantaranya: cara memperoleh data pengguna TikTok dan cara mengungkapkan isinya. Seperti teman dan pengikut, dengan siapa pengguna berkomunikasi. Kekurangan dari penelitian ini adalah waktu dalam analisis *file* XML, dari 103 *file* XML akan lebih baik bila dibuat sebuah ciri-ciri sehingga mempermudah dalam menentukan *file* yang berkaitan dengan kebutuhan.

Teknis penelitian berikutnya berbeda, yaitu dengan menggunakan module 2 fungsional pesan dan kontak untuk Android Analyzer Autopsy. Peneliti juga menggunakan file XML untuk mendukung analisa. OS yang dianalisis hanya khusus untuk Android. Kesimpulannya walaupun sesama sistem operasi android hasil file XML dapat berbeda. Pengembangan dapat dilakukan pada modul dengan menambahkan fungsionalnya (Domingues et al., 2020).

Tabel 1.1 Ulasan Kritis

No	Penelitian	Tahapan	Metode	*File*	Aplikasi	Hasil
1	Anglano, C. (2014)	• Menggunakan Emulator Youwave • Identifikasi • Ekstraksi • Analisa Data	Analisis data dengan skenario eksperimen	• vm01.vdi • whatsapp.log, whatsapp-<date>.log • UID.j • wa.db	Whatsapp	Menemukan bahwa antara emulator dan perangkat sungguhan memiliki kriteria barang bukti sama kuat seperti: database kontak, database obrolan, *backup* database *chat*, *avatars of Contacts*, *copies of contacts avatars,* ***log files, received files, sent files dan user settings and preferences*.**
2	Ali, A., & Fazeel. (2016)	• *Identification and collection* • *Preservation* • *Examination and analysis* • *Presentation*	NIST	• UID.j • *Login* • *User Information* • *FriendList* • *Post* • *Messaging* • *Comment*	Facebook, Twitter, LinkedIn and Google+	Hasilnya dapat membuat kriteria barang bukti dari setiap sistem operasi. Tetapi, melakukan kajian pada artefak Android tidak dijelaskan lebih rinci nama dan jenis file. Berbeda dengan iOS, peneliti menjelaskan semua kriteria dari berkas yang di ekstraksi.
3	Anglano, C., Canonico, M., &	• *completeness* • *repeatability* • *generality*	Designing suitable experiments	• cache4.db • *userconfing.xml* • *cache*	Telegram	Penelitian ini menghasilkan normalisasi dari database sehingga memudahkan dalam menentukan kebutuhan barang bukti. Pada tabel *user* di rekonstruksi dengan tabel *contact,* tabel *accounts* dengan tabel

No	Penelitian	Tahapan	Metode	*File*	Aplikasi	Hasil
	Guazzone, M. (2017)			• *media*		*raw_contacts* dan tabel *dialogs* dengan tabel *messages*.
4	Cedillo, P., Camacho, J., Campos, K., & Bermeo, A. (2019)	• *identification* • *collection* • *analysis* • *preservation*	ISO/IEC 27037:2012	• xlsx	Microsoft Excel	Penelitian ini menyelesaikan tujuan berikut: • Mendeteksi dan menghitung jumlah file menurut jenisnya. • Menentukan jumlah lembar, kolom dan baris dalam file Microsoft Excel dan jumlah baris dalam file teks. Aktivitas ini dilakukan untuk menunjukkan panjang setiap file. • Mendapat kolom yang berisi tanggal dan waktu aktivitas pengguna. • Membandingkan tanggal yang dimasukkan oleh penyidik forensik dengan tanggal pembuktian. • Menyimpan data yang difilter.

No	Penelitian	Tahapan	Metode	*File*	Aplikasi	Hasil
						• Menggabungkan data dalam satu file. • Menyusun data dalam urutan menurun, sehingga tersusun secara kronologis. • Menghapus data berulang. • Menetapkan kode untuk setiap aktivitas. • Menyimpan laporan.
5	Hoang Khoa, N., The Duy, P., Do Hoang, H., Thi Thu Hien, D., & Pham, V. H. (2020)	• *Identification* • *Acquisition* • *examination* • *reporting*	DFRWS (Digital Forensics Workshop) Investigative Model	• video.db • applog_stats. xml • aweme_user. xml • downloader.db • *db_im_xx.db*	TikTok	Mendapatkan Analisa terhadap Sistem Operasi Android untuk melihat artefak yang tertinggal yang mana ditemukan file XML serta database aplikasi TikTok seperti informasi user, *log* aplikasi, database video, *downloader* dan *user*.
6	Domingues , P., Nogueira, R., Francisco, J. C., &	• *identification* • *analysis* • *Creation Modul*	Perbandingan *Non-Private Data* dan *Private Data*	• db_im_xx • lib_log_queue.db • video.db	TikTok	Penelitian ini menguraikan hasil database ke dalam 2 fungsional modul diantaranya fungsional kontak juga pesan dan pengkajian pada 4 berkas XML.

No	Penelitian	Tahapan	Metode	*File*	Aplikasi	Hasil
	Frade, M. (2020)			• *aweme_user.xml* • *search.xml* • *appsflyer-data.xml*		
7	Usulan	• *identification and collection* • *preservation* • *analysis* • *presentation*	Analysis DFXML and Development MAP	• localHashTag.db • video • downloader.db • ss_app_log.db • aweme_local_video.xml • Search.xml • Aweme_user.xml • description.info.xml	TikTok	DFXML digunakan pada analisis berkas XML aplikasi TikTok di Android untuk memetakan karakteristik bukti digital yang relevan jika terdapat lebih dari satu akun agar tidak banyak memakan waktu dalam pengujian, memetakan berkas penting untuk investigasi pada aplikasi TikTok.

No	Penelitian	Tahapan	Metode	*File*	Aplikasi	Hasil
				• custom_channels.xml • LoginSharePreferences.xml • publish.xml • traffic_monitor_info.xml • version.xml		

1.7 Metode Penelitian

Penelitian ini membutuhkan tahapan untuk mempermudah agar menjadi teratur dan mendapatkan hasil yang maksimal. Berikut gambaran umum mengenai langkah-langkah yang akan dilakukan.

1. Tinjauan Pustaka

Tinjauan pustaka dilakukan untuk mengetahui informasi seputar penelitian. Jurnal penelitian terkait, dokumen presentasi, bahan bacaan dari buku dan berita tentang kasus-kasus di TikTok. Tinjauan dilakukan supaya terhindar dari penelitian plagiasi dan mengetahui poin-poin yang pengembangan terhadap penelitian sebelumnya.

2. Persiapan Sistem

Melakukan persiapan yang dibutuhkan untuk mendukung penelitian ini seperti analisis kebutuhan diantaranya pengelompokan perangkat, pengelompokan akun pelaku dan korban juga bahasa pemrograman Python dalam membuat modul.

3. Skenario dan Simulasi Kasus

Tahapan ini merupakan membuat simulasi kasus dalam sebuah telepon pintar memiliki empat akun tetapi hanya menggunakan tiga akun saja saat melakukan kejahatan. Akun pertama melakukan postingan video SARA, akun kedua melakukan pelecehan secara verbatim mengirim pesan lalu menghapusnya dan akun ketiga melakukan postingan video hoax kemudian menghapus akunnya.

4. *Identification, Collection dan Preservation*

Identification Tahap ini merupakan proses identifikasi dilakukan untuk menentukan kebutuhan apa saja yang diperlukan pada penyelidikan dan pencarian barang bukti. *Collection* melakukan proses pengumpulan identifikasi bagian yang khusus dari barang bukti digital dan melakukan identifikasi sumber data. *Preservation* Tahap ini merupakan tahap pemeliharaan dilakukan untuk menjaga barang bukti digital, memastikan keaslian barang bukti dan menyangkal klaim bahwa barang bukti telah dilakukan perubahan atau sabotase.

5. Analisa Menggunakan DFXML

Hasil dari penentuan *file* akan di analisis menggunakan DFXML untuk dikaji dari masing-masing akun sehingga menghasilkan pemetaan karakteristik barang bukti digital yang relevan.

6. Hasil Pembahasan dan Laporan

Laporan penelitian ini yaitu semua kegiatan yang dilakukan akan dituangkan untuk di dokumentasi apapun hasilnya, baik kelebihan maupun kekurangan metode yang diterapkan.

Sehingga penelitian berikutnya dapat menggunakan hasil penelitian ini sebagai bahan acuan ataupun referensi.

1.8 Sistematika Penulisan

Tahapan berikut memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematik penulisan sebagai berikut:

BAB I Pendahuluan

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian serta sistematik penulisan.

BAB II Tinjauan Pustaka

Pada Bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang berkaitan dengan penelitian yang sedang diteliti.

BAB III Metodologi Penelitian

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta perancangan antar muka aplikasi yang akan dibuat.

BAB IV Pembahasan

Pada Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis dan evaluasi dari penelitian yang diangkat.

BAB V Penutup

Pada bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutny.

BAB 2
Tinjauan Pustaka

2.1 Penelitian Terdahulu

Penelitian (Anglano, 2014), analisis *database* pada kontak untuk merekonstruksi daftar kontak di aplikasi WhatsApp *Messenger.* Hasilnya penyelidik dapat menemukan ketika kontak telah ditambahkan, memulihkan kontak yang dihapus dan menemukan waktu penghapusannya. Korelasi dengan pesan yang dikirim penyidik dapat mengidentifikasi pesan yang telah dihapus dan kapan pesan tersebut dikirim. Penelitian ini menggunakan Emulator Android YouWave yang menjalankan Android versi 4.4.4 sebagai lingkungan analisisnya. Penelitian pada emulator ada yang tidak dapat di ekstraksi yaitu posisi (GPS). Sebab, tidak memungkinkan karena emulator yang digunakan tidak mendukung. Sehingga *region* di *file log* tidak tersedia.

Penelitian Ali & Fazeel (2016), identifikasi artefak digital pada aplikasi *Facebook*, *Twitter* dan *LinkedIn* di sistem operasi Android, iOS, Windows dan BlackBerry. Cara yang digunakan adalah ekstrak *disk image* selanjutnya melakukan analisis pada berkas *database*. Semua aplikasi yang diuji memiliki karakteristik yang berbeda setiap sistem operasi, tantangannya semakin hari akan semakin banyak media sosial yang perlu di analisis.

Peneliti Anglano dkk (2017), dapat mengidentifikasi semua artefak Telegram *Messenger* di Android. Secara khusus, peneliti telah membahas metode untuk menafsirkan data yang disimpan dalam *database* dan *file* konfigurasi pengguna. Hasilnya dapat merekonstruksi daftar kontak, pesan tekstual dan non-tekstual yang dipertukarkan serta menentukan apakah pengguna membuat atau mengelola obrolan rahasia, grup dan saluran.

Cedillo dkk (2019) penelitian tentang *Log Activity*. Hasilnya, dapat melihat aktivitas yang dibagi menjadi 5 jenis: riwayat penelusuran web, *cookie*, gambar, unduhan, dan *instan messenger.* Adapun riwayat penjelajahan, 11 halaman web ditemukan. Sedangkan untuk *cookie* ada 8 aktivitas, kemudian 4 gambar yang dapat dipulihkan. *File* PDF ditemukan dalam aktivitas unduhan dan pesan audio pada aplikasi WhatsApp.

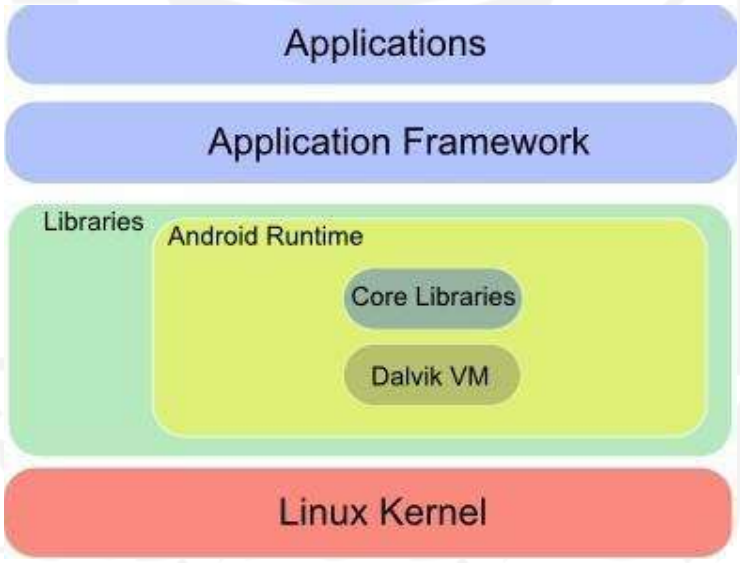
Metode penelitian (Hoang Khoa et al., 2020) adalah dengan menganalisis artefak yang tertinggal di telepon pintar Android. Hasilnya, menjawab pertanyaan secara umum diantaranya: cara memperoleh data pengguna TikTok dan cara mengungkapkan isinya. Seperti teman dan pengikut, dengan siapa pengguna berkomunikasi. Kekurangan dari penelitian ini

adalah waktu dalam analisis *file* XML, dari 103 *file* XML akan lebih baik bila dibuat sebuah ciri-ciri sehingga mempermudah dalam menentukan *file* yang berkaitan dengan kebutuhan.

Teknis penelitian berikutnya berbeda, yaitu dengan menggunakan module 2 fungsional pesan dan kontak untuk Android *Analyzer* Autopsy. Peneliti juga menggunakan *file* XML untuk mendukung analisa. OS yang dianalisis hanya khusus untuk Android. Kesimpulannya walaupun sesama sistem operasi android hasil *file* XML dapat berbeda. Pengembangan dapat dilakukan pada modul dengan menambahkan fungsionalnya (Domingues et al., 2020).

2.2 Android

Menurut (Döring & Wei, 2012) Android adalah perangkat lunak *open source*. Umumnya setiap versi baru sistem operasi Android dikembangkan dengan Nama kode berdasarkan item makanan penutup sampai pada versi Android 9.0 Pie. Selanjutnya bernama Android 10 atau Android Q. Arsitektur Android dikembangkan dengan tujuan untuk membuat ponsel yang lebih baik bagi konsumen dipimpin oleh OHA (*Open Handset Alliance)* Arsitektur dari Android dapat dilihat pada gambar 2.1.



Gambar 2.1 Arsitektur Android (Sumber (Döring & Wei, 2012))

Menurut Sheikh dkk (2013). Sistem dasar arsitektur Android adalah kernel Linux 2.6 yang mendukung *security*, *memory management*, *process management*, *network stack and device driver model*.

Penelitian (Al-Dhaqm et al., 2017) memperkenalkan tahapan untuk mengumpulkan barang bukti dari perangkat Android. Metode yang mereka gunakan terdiri dari Lima proses investigasi sebagai berikut: *identifying the device and preserving the evidence, collecting the evidence, examining and analyzing, and reporting and presentation.*

Akuisisi fisik dan logis perangkat Android menggunakan dd (Norouzizadeh Dezfouli et al., 2016)melakukannya dengan alat forensik seluler seperti Cellebrite UFED atau dengan *booting* ke *recovery mode*. Akses *superuser* untuk mengambil *image* dari setiap *file* mtd yang ada di direktori / dev / mtd. Akuisisi logis menggunakan Cellebrite UFED untuk mengekstrak data dari / data / data. Sementara *booting* ke *recovery mode* dapat digunakan saat perangkat dimatikan dan ingin menghindari untuk menyalakan perangkat. Penelitian (Kim & Lee, 2020) menemukan tindakan pengguna dalam *log* file, SQLite *database file* yang berisi informasi penting dari perspektif forensik seperti ID, Kontak, Geodata, dan *Message* dan termasuk *timestamp* pada Android.

2.3 File XML

Menurut (Garfinkel, 2012) keunggulan *File* XML lebih mudah untuk berbagi data karena *file* jauh lebih kecil daripada *disk image*. Atribut XML secara ekstensif membutuhkan aturan penguraian yang kompleks, pendekatan dalam mengurai *file* XML yaitu *Digital Forensic* XML (DFXML). Hasil dari DFXML berisi dokumentasi asal data, tempat program aplikasi dikompilasi, pustaka yang ditautkan, lingkungan *runtime*, lokasi fisiknya dalam *image disk* (dalam kasus PhotoRec) dan hash kriptografi nya.

Menurut (Laurenson et al., 2015) DFXML dipilih karena memenuhi persyaratan untuk mengidentifikasi APXM (*Application Profile* XML). Gambar 2.2. Contoh kerangka dari struktur APXML.

```
<?xml version='1.0' encoding='UTF-16'?> <apxml version="'1.0.0'"
xmlns="https://github.com/thomaslaurenson/apxml_schema" xmlns:dc="http://purl.org/dc/elements/1.1/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:delta="http://www.forensicswiki.org/wiki/Forensic_Disk_Differencing"> <metadata/> <creator/>
<install> <!-- DFXML FileObjects --> <!-- RegXML CellObjects -->
</install> <execute> <!-- DFXML FileObjects --> <!-- RegXML CellObjects -->
</execute> <uninstall> <!-- DFXML FileObjects --> <!-- RegXML CellObjects -->
</uninstall> </apxml>
Figure
```

Gambar 2.2 Contoh Kerangka *Application Profile* XML (APXML) (Sumber (Laurenson et al., 2015)).

Uniform Resource Identifier (URI) berfungsi sebagai penentu *namespace* APXML: *https://github.com/thomaslaurenson/apxml_schema*. *Schema* artinya memberikan kepatuhan terhadap konvensi penamaan elemen unik dalam dokumen APXML (Laurenson et al., 2015).

Penelitian Hoang Khoa dkk (2020) dapat mengumpulkan informasi dalam *file* XML pada direktori *shared_prefs* sebagai berikut: *The first opening time of the application, The installation time of the application, The last time that the application is updated, The MAC address of the last connected SSID, Recent searching history, Language* dan *Region.* Contoh gambar 2.3 adalah *file* bernama applog_stats.xml memberikan beberapa informasi seperti *device ID*, *MAC address of last connected* SSID, *timestamp of the last* SSID *connection.*

Gambar 2.3 Contoh File Applog_stats.xml (Sumber (Hoang Khoa et al., 2020)).

2.4 Database *SQLite*

Salah satu aplikasi yang menjadikan *SQLite* sebagai penyimpanan adalah *Instant Messenger* dan sebagian besar *browser* di perangkat seluler. Luasnya kecocokan dari *SQLite* sebagai penyimpanan telah mengarah pada situasi forensika digital karena memerlukan analisis dari data yang disimpan dalam database *SQLite* (Nemetz et al., 2018).

Menurut (Musleh et al., 2018) *SQLite* menyediakan *SQL syntax, transactions and prepared statements*. Seperti database lainnya, *SQLite* mendukung tipe data seperti *TEXT*, *INTEGER* dan *REAL*. *SQLite* merupakan database relasional yang ringan pada OS Android secara *default*. Saat *developer* membuat database *SQLite* menggunakan Android SDK,

mereka perlu memahami komponennya. Pertama, *SQLiteDatabase* adalah *main class* untuk database *SQLite*. Kemudian *Class* tersebut merupakan buka tutup koneksi *database*.

Pada analisis artefak database, peneliti (Walnycky et al., 2015) menemukan bahwa *TextMe* dan *Nimbuzz* memakai *SQLite Database* penyimpanan data sensitif pengguna termasuk nama pengguna, email, nomor telepon, tanggal lahir, dan kata sandi pengguna dalam teks biasa. Berikut gambar *TextMe's database* dengan *user data* dalam *plaintext*.

	id	key	value
	Filter	Filter	Filter
1	24	database.migration	3
2	47	user.username	unhcfregdroid
3	48	user.email	[redacted]@live.com
4	49	user.phone	+1203[redacted]
5	50	user.sms_number	+1914[redacted]
6	51	user.gender	m
7	52	user.birthday	1992/07/22
8	53	user.password	gin[redacted]
9	54	user.password_hashed	false
10	55	user.userId	47763570

Gambar 2.4 *TextMe's database dengan user data* dalam *plaintext* (Sumber (Walnycky et al., 2015)).

Peneliti (Walnycky et al., 2015) mengungkapkan bahwa ada indikasi pengiriman *Screenshot* pengguna aplikasi *TextMe's* kepada pihak ketiga, tetapi jika dilihat dari tangkapan lalu lintas jaringannya tidak ada terdeteksi pengiriman dari telepon pintar pengguna.

2.5 TikTok

TikTok adalah salah satu aplikasi terpopuler di dunia dengan ratusan juta pengguna, aplikasi ini memiliki reputasi pertumbuhan tercepat dan menempati peringkat aplikasi ketujuh yang paling banyak diunduh dalam dekade terakhir. Fitur TikTok adalah mengunggah, menonton, dan menjelajahi video dan *meme lip sync*. TikTok memberikan hak penggunanya untuk mengunggah video *lip-sync* hingga 60 detik dengan berbagai fitur kreatif dan interaktif (Weimann & Masri, 2020).

Menurut (Wang et al., 2019) TikTok memiliki fitur kontrol audio dan visual untuk membuat video berdurasi 15 detik, fitur ini mencakup *in-camera speed controls, image-tracking composites, collaborative split-screens,* dan *a shortened video timeline*. Fitur selanjutnya meneruskan konten video ke teman mereka di TikTok. Mereka juga dapat

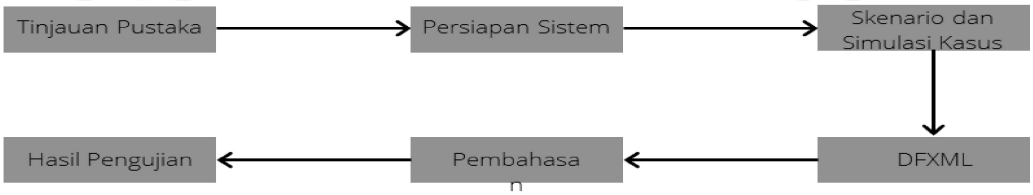
meneruskan video ke media sosial lain. Menurut (Bresnick, 2019), TikTok dapat diibaratkan taman bermain anak yang kelahiran 2010-an. Karena struktur taman bermain dalam bentuk virtual. Disimpulkan ada 4 faktor alasan TikTok sangat populer di kalangan anak muda diantaranya *Playback Speed, Face-Replacement and Augmented Reality*, *Audio Visual Remixing* dan *Chronological sequencing and montage.*

Menurut (Yu, 2019) aplikasi TikTok sangat disukai karena memiliki desain antarmuka dan interaktif yang dapat menyesuaikan dengan selera penggunanya. Konten yang didistribusikan memiliki ketergantungan pada informasi data serta algoritma kecerdasan buatan. Aplikasi ini menerapkan beberapa model untuk membuat visual kontennya terlihat beragam tetapi stabil berdasarkan selera, model tersebut adalah UGC (*User-Centered Design*), PGC (*Professionally Generated Content*) dan OGC (*Occupationally Generated Content*).

BAB 3
Metodologi

3.1 Alur Metodologi Penelitian

Tahapan metodologi yang diusulkan menjelaskan bagaimana cara penelitian ini dilakukan sehingga dapat diketahui rincian tentang langkah-langkah yang dibuat secara sistematis, membuat analisis terhadap hasil penelitian serta kesulitan-kesulitan yang dihadapi. sehingga dapat dijadikan sebagai pedoman yang jelas dalam menyelesaikan permasalahan. Adapun langkah-langkah pada penelitian ini dapat dilihat pada Gambar 3.1.



Gambar 3.1 Alur Metode Penelitian

Metode penelitian ini memiliki 7 tahapan yakni (1) Tinjauan Pustaka (2) Persiapan Sistem (3) Skenario dan Simulasi Kasus (4) Analisis Menggunakan DFXML (5) Pembahasan dan (6) Hasil Pengujian.

3.2 Tinjauan Pustaka

Tinjauan Pustaka dilakukan untuk mengetahui informasi seputar penelitian. Fokus membaca penelitian terkait, jurnal penelitian sebelumnya, dokumen presentasi, bahan bacaan dari buku juga kasus-kasus dari berita online. Tinjauan dilakukan supaya terhindar dari penelitian plagiasi dan mengetahui poin-poin yang dapat dikembangkan terhadap penelitian sebelumnya.

3.3 Persiapan Sistem

Persiapan Sistem, tahapan ini mempersiapkan segala hal yang dibutuhkan dalam penelitian seperti kebutuhan pengelompokan perangkat, pengelompokan akun pelaku dan korban. Menggunakan bahasa pemrograman java dalam membuat modul, identifikasi DB yang diperlukan untuk diurai agar dapat divisualisasikan ke dalam XML.

3.3.1 Pengelompokkan Perangkat

Pengelompokan Perangkat terdiri dari dua hal yakni perangkat keras dan perangkat lunak, perangkat-perangkat ini digunakan sebagai penunjang dalam melakukan simulasi eksperimen kejahatan dan investigasi. Spesifikasi lanjut dapat dilihat sebagai berikut.

1. Perangkat Keras

Perangkat yang digunakan ada sebagai alat pelaku dan alat investigator yaitu:

a. Redmi 5A spesifikasi RAM 2 GB, CPU Quad-Core 1.40 GHz dengan Penyimpanan 16 GB.
b. Investigator memiliki laptop Dell latitude e7240 dengan spesifikasi Windows 10 Pro 64-bit, Intel Core i5-4310U dengan kecepatan Frekuensi up to 2.6 GHz, RAM 8 GB dan SSD 250 GB sebagai alat melakukan penggalian dan analisis barang bukti.

2. Perangkat Lunak

Perangkat lunak yang digunakan memiliki spesifikasi:

a. Sistem Operasi Android versi Oreo 10.0.
b. TikTok versi 16.0.41 untuk Android (4 akun).
c. Pemrograman Python.
d. Android backup Mobiledit.
e. AccessData FTK Imager.
f. Hash Tool 1.2.1.
g. Autopsy 4.14 untuk menjalankan fungsional modul.
h. DB Browser untuk membaca SQLite3 Database.

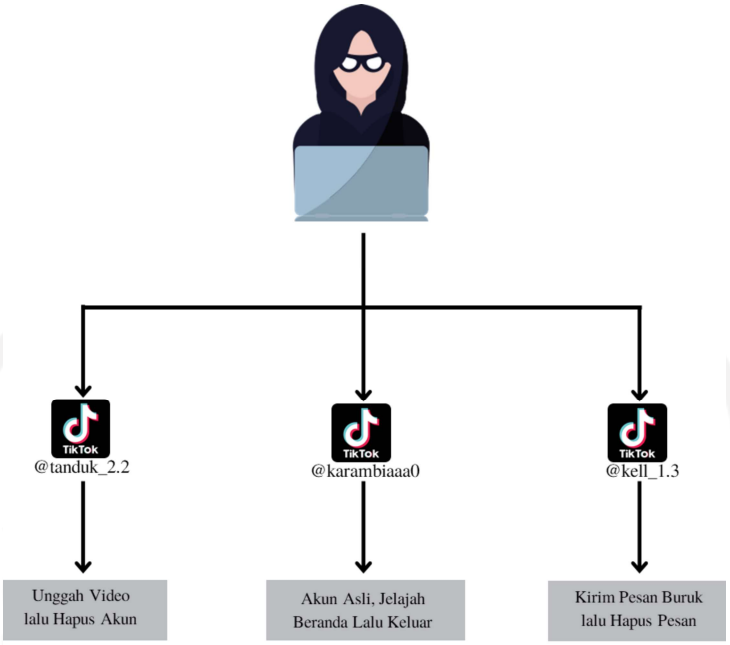
3.3.2 Pengelompokan Akun TikTok

Penelitian ini dilakukan dengan membuat eksperimen yang melibatkan lebih dari satu akun diantaranya:

a. @kell_1.3 Kasus video SARA dan mengirim pesan lalu menghapusnya.
b. @tanduk_2.2 kasus postingan video hoax kemudian menghapus akunnya.
c. @karambiaaa0 akun terakhir sebagai akun asli dari pelaku.
d. @muhammadromi_0.1 target.

3.4 Skenario dan Simulasi Kasus

Tahap ini membangun sebuah skenario dan simulasi kasus agar penelitian ini dapat berjalan layaknya di kehidupan nyata, gambar 3.2 merupakan simulasi.



Gambar 3.2 Skenario Kasus

Skenario dan simulasi kasusnya pada telepon pintar Android dengan perangkat Xiaomi Redmi 5. Dipasang aplikasi TikTok versi 16.0.41. Kemudian masuk menggunakan akun yang asli milik pelaku dengan *username* @karambiaaa0 dan tidak melakukan apa-apa, akun hanya berfungsi sebagai penanda dalam skenario kasus.

Akun selanjutnya yang masuk adalah *username* @kell_1.3 melakukan simulasi kegiatan pada aplikasi TikTok seperti menggunakan fitur pencarian, melihat video pada beranda, membuat video SARA dengan konten menjelekkan sebuah agama dan mengunggahnya. Selanjutnya melakukan kegiatan pengiriman pesan, akun @kell_1.3 mengirimkan sebuah pesan kepada @muhammadromi_0.1 dengan pelecehan secara verbatim, kemudian pada perangkat yang dipakai pelaku pesan tersebut dihapus dengan maksud menghilangkan jejak.

Akun yang masuk selanjutnya adalah *username* @tanduk_2.2, akun ini sedikit unik karena melakukan kegiatan unggahan video hoax. Video tersebut diunggah dengan konten memberikan informasi palsu, kemudian pelaku menghapus akunnya.

3.5 Lokasi Berkas

Total berkas XML lebih dari 200, berkas tersebut secara acak terletak di seluruh folder. Sebelum melakukan analisis DFXML, lokasi dari seluruh berkas XML harus dibuat agar dapat dipilih untuk penelitian.

3.6 Analisis Menggunakan DFXML

Penelitian pada tahap ini menganalisis *file* XML dari aplikasi TikTok tentang versi aplikasi yang dipakai, *applog*, *login, user, custom channels*, pencarian serta dimasukkan informasi lain yang dianggap penting nantinya. Sebagai gambaran *file* XML yang dianalisis pada bagian pencarian seperti gambar 3.3 kode berikut.

```
<map> <string name="place_holder">Search</string>
<string
name="recent_history">[{&quot;keyword&quot;:&quot;hay trao cho
anh&quot;,&quot;int&quot;:0},{&quot;keyword&quot;:&quot;b e
sa&quot;,&quot;int&quot;:0}]</string>
</map>
```

Gambar 3.3 *Search.xml* (sumber (Hoang Khoa et al., 2020))

Sebagai informasi fitur pencarian pada aplikasi TikTok tidak secara aktif memberikan ke target yang diinginkan melainkan secara masif, hasil yang ditampilkan adalah video keterkaitan dengan kata pencarian yang digunakan. Gambar 3.3 pengguna menggunakan pencarian dengan riwayat Dua kali yaitu hai traoi cho anh dan b e sa.

3.7 Pembahasan

Tahap ini merupakan pembahasan artefak dari DFXML serta gambaran visual dari modul plugin pada perangkat lunak Autopsy yang dikembangkan.

3.8 Hasil Pengujian

Pengujian nantinya akan ada beberapa tabel yang memetakan hasil dari masing-masing tahapan dalam proses investigasi forensik dapat dilihat seperti pada tabel 3.2 informasi *file* XML TikTok dan tabel 3.3 Fitur yang dapat diidentifikasi.

Tabel 3.1 Informasi *file* XML TikTok

No	Nama *File*	Akun		
		@karambiaaa	@kell_1.1	@tanduk_2.2
1				
2				
3				
4				
n				

Keterangan

Nama *File* merupakan berkas berekstensi .xml

Akun merupakan segala informasi setiap akun dari *file* .xml

Tabel 3.2 Kebutuhan Berkas untuk Analisis

No	Nama Berkas	Status Kebutuhan Analisis		
		Sangat	Kurang	Tidak
1				
2				
3				
4				
n				

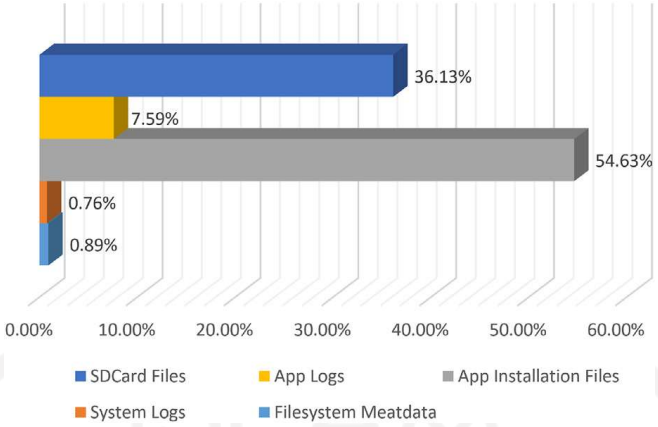
BAB 4
Hasil dan Pembahasan

4.1 Tinjauan Pustaka

Menurut (Laurenson et al., 2015) Sistem Berkas XML adalah Abstraksi data yang disesuaikan untuk distribusi profil aplikasi yang dirancang dalam menentukan struktur, skema klasifikasi, penyertaan properti metadata terkait dan standardisasi. Berkas XML digunakan dalam banyak hal sebagaimana penelitian (Oliveira et al., 2020) menemukan beberapa sistem mengadopsi XML (eXtensible Markup Language) untuk merepresentasikan data semi-terstruktur. Banyak industri dan komunitas ilmiah telah mengadopsi dokumen XML sebagai standar untuk merepresentasikan, menyimpan, dan bertukar data. Akibatnya, sejumlah besar dokumen XML dibuat setiap hari. Contohnya termasuk aplikasi, bagian perawatan kesehatan dan lain-lain. Selain itu, Dewan Riset Nasional Brasil (CNPq) mewajibkan setiap peneliti untuk menyimpan kurikulum mereka di *platform Lattes* yang menggunakan XML sebagai formatnya.

Penelitian (Brahmia et al., 2020) mengungkapkan bahwa XML memberikan dukungan yang sangat baik untuk model data yang dikelompokkan secara temporer, yang dianggap sebagai representasi informasi temporal yang paling alami dan efektif. Berkas XML digunakan juga dalam telepon pintar sebagai *System Logs.*

Menurut penelitian (Kim & Lee, 2020) dalam mengelola berkas yang berisi bukti potensial di Android berdasarkan perilaku tersangka. Terdiri dari metadata sistem berkas dan nilai hash *Merkle-tree* dari file yang terkait dengan setiap tindakan menggunakan struktur XML. *Potential Evidence Groups* (EPGs) diuraikan dengan mengurangi rasio positif palsu untuk grup yang salah diidentifikasi melalui dua proses: Pertama, mengklasifikasikan file berdasarkan *Signature* dan menemukan grup yang berisi file dengan format yang harus dianalisis sesuai dengan jenis investigasi, kedua analisis melalui berkas berformat SQLite. Klasifikasi PEGs dari Android.



Gambar 4.1 Klasifikasi *Potential Evidence Groups (PEGs)* (Sumber (Kim & Lee, 2020))

4.2 Elemen Standar Informasi Sistem Berkas (XML)

Menurut (Garfinkel, 2012) Sistem berkas metadata adalah nama yang diberikan untuk informasi dalam sistem berkas selain konten berkas, termasuk nama berkas, stempel waktu, daftar kontrol akses, dan label disk. Sistem berkas metadata banyak digunakan dalam forensik komputer sebagai alat utama untuk menavigasi informasi sistem berkas dan merekonstruksi *timelines* termasuk format yang berisi 16 entri untuk setiap berkas termasuk nama berkas, ukuran, waktu MAC, status alokasi, dan metadata lain yang dapat dipulihkan dari sistem berkas.

Penelitian (Ikhsani & Hidayanto, 2016) menemukan komponen metadata dalam bentuk ekstensi .db, terdapat banyak elemen di dalamnya seperti *timestamp, created, status, regional, type, content, sent, read* dan lainnya. Penelitian (Riley, 2017) XML (*eXtensible Markup Language*) adalah sebagai pengkodean, transfer, dan mekanisme penyimpanan sistem internal yang umum digunakan untuk metadata. Metadata dalam XML sebagai kumpulan file, XML yang mendefinisikan 15 elemen diantaranya *contributor, specific information, identifier, creator, description, publisher, date/time, type, title / name of file, format, source, language, relation, coverage dan right.* Menandakan bahwa nilai-nilai di dalamnya memiliki arti tertentu dan dari fitur inilah dokumen XML mendapatkan strukturnya. Dokumen XML seperti pohon yang memiliki akar tunggal. Kemudian memiliki cabang dari elemen dan nilai lain, membentuk sebuah struktur yang berkontribusi pada makna nilai metadata dalam dokumen. Atribut XML dan nilainya memperhalus makna elemen di mana atribut tersebut muncul. XML mendukung multi bahasa metadata dengan menyediakan atribut yang telah ditentukan sebelumnya untuk menunjukkan bahasa di mana

nilai elemen muncul. Seperti database relasional sebagai dokumen XML yang menjelaskan atau dikenal penafsiran catatan metadata.

Komponen terpenting dalam metadata menurut paparan (Wawrzyniak & El Fray, 2020) adalah *General signature* dan *signature validation. General signature* memiliki 2 komponen yaitu *Creation of References* menjelaskan tentang sumber lokasi unduh via URI, melakukan transformasi yang dijelaskan dalam elemen transform pada objek data yang dirujuk dan menggunakan algoritma untuk menghitung nilai fungsi hash. Kemudian *Signature creation* komponennya *"SignedInfo"* (termasuk elemen referensi), nilai hash *"SignedInfo"* dan enkripsi nilai hash lalu disimpan pada *"SignatureValue. Signature validation* juga memiliki 2 komponen yaitu *reference validation* mengeksekusi algoritma perhitungan hash untuk menghitung nilai hash dari dokumen yang diubah dan *signature validation* melakukan pembacaan informasi kunci dari *"KeyInfo"* kemudian menjelaskan tentang *"Signature Value"* dari *"Signature Method".*

Elemen XML yang ditemukan oleh (Hoang et al., 2016) seperti VTs dan VTe untuk waktu validasi, atribut timestamp TTs dan TTe untuk waktu transaksi, kontributor, *identifier, coverage* dan *right, title / name of file, format, , language, source, relation, creator* dan *data type.* Hampir sama dengan penelitian (Brahmia et al., 2020) Konvensional XML memiliki elemen informasi dari pembuat seperti nama dokumen berekstensi, XSD (*XML Schema Definition*) artinya definisi dari tujuan kode yang dibuat, *contributor, publisher, specific information, identifier*. Elemen yang paling utama adalah *TST (Transaction Start Time) dan TET (Transaction End Time)* atau dapat disebut *Timestamp* yang sudah termasuk validitasnya (VST dan VET).

Tabel 4.1 Elemen Standar Informasi Sistem Berkas XML

No	Nama Elemen	Keterangan
1	uid	ID pengguna yang memiliki file. Numerik dalam sistem file POSIX tetapi string untuk SID di NTFS.
2	Version	Versi program penghasil XML.
3	Start Time	Tanggal dan waktu program dijalankan.
4	OS Version	Versi sistem operasi yang digunakan dalam membuat berkas XML
5	Atime	Waktu terakhir diakses.
6	Crtime	Waktu dibuat
7	Ctime	Waktu metadata dimodifikasi
8	Dtime	Perekaman saat dihapus
9	Mtime	Waktu dimodifikasi
10	Username	Nama Pengguna saat program dijalankan

11	Name_type	Representasi tipe berkas seperti umum, direktori, pranula dan lain-lain

4.3 Persiapan Sistem

Langkah teknis pertama dalam penelitian ini adalah mempersiapkan sistem yang akan digunakan pada proses analisis. Tahapan awal adalah membuat pengelompokan perangkat dan Akun.

4.3.1 Pengelompokan Perangkat

Pengelompokan pada tahapan ini memiliki dua bagian yaitu perangkat keras dan lunak. Peralatan yang perlu dipersiapkan antara lain:

Tabel 4.2 Spesifikasi perangkat lunak dan perangkat keras

No	Perangkat Lunak/Keras	Keterangan
1	Dell latitude e7240	Perangkat Keras
2	Redmi 5A MIUI 11	Perangkat Keras
3	Micro USB Connector Original OPPO	Perangkat Keras
4	Windows 10 Pro 64-bit	Perangkat Lunak
5	Android versi Oreo 10.0	Perangkat Lunak
6	TikTok versi 16.0.41	Perangkat Lunak
7	Phyton	Perangkat Lunak
8	Autopsy 4.14	Perangkat Lunak
9	DB Browser (SQLCipher) 3.12.1	Perangkat Lunak
10	AccessData FTK Imager 4.2.1.4	Perangkat Lunak
12	Android Backup Mobiledit 7.3.0.19270	Perangkat Lunak
13	Notepad++ 7.9.1	Perangkat Lunak
14	Hash Tool 1.2.1	Perangkat Lunak

4.3.2 Pengelompokan Akun

Penelitian ini dilakukan dengan membuat eksperimen yang melibatkan lebih dari satu akun diantaranya:

Tabel 4.3 Pengelompokan akun

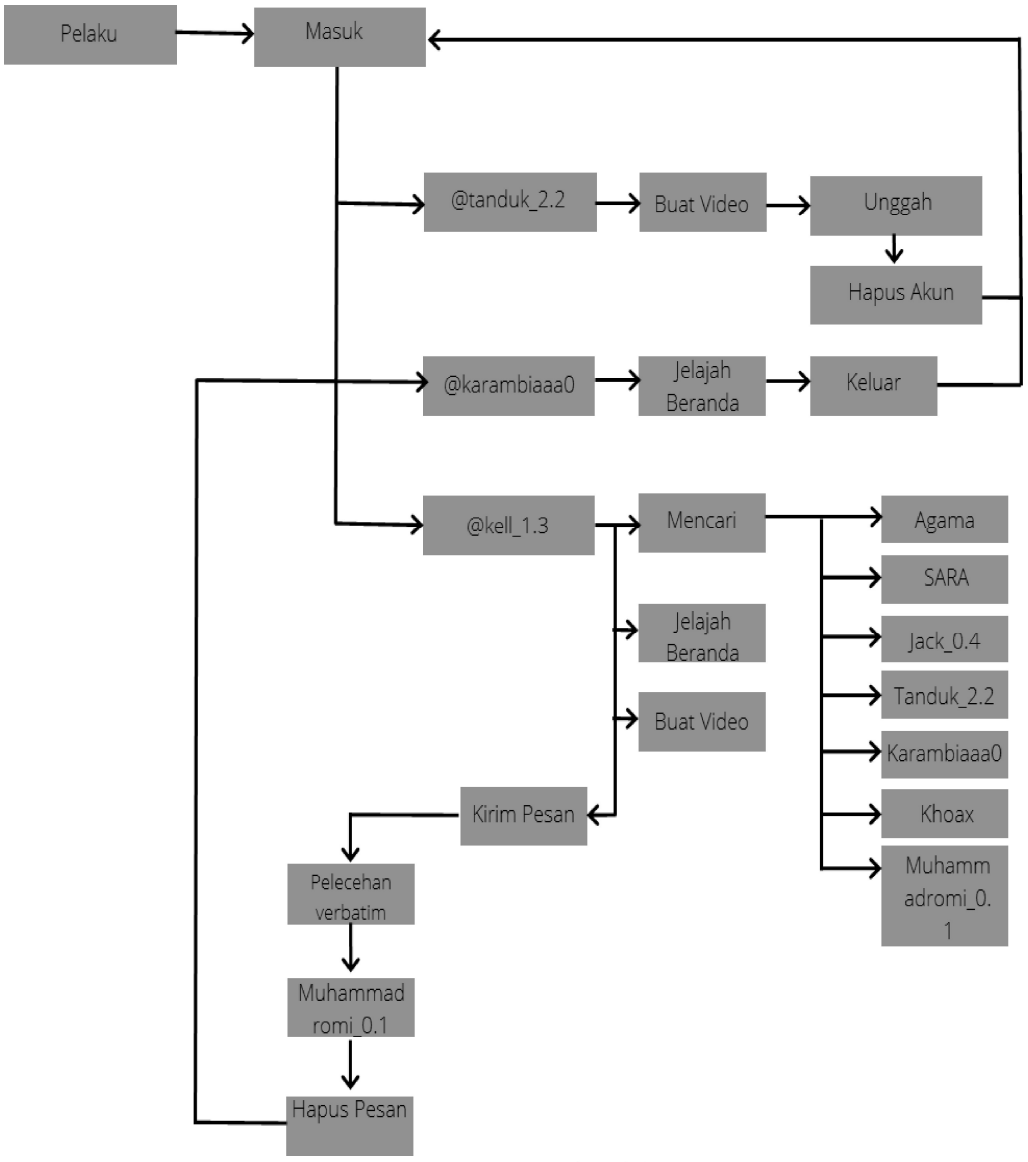
No	Akun	Keterangan
1	@kell_1.3	Video SARA dan mengirim pesan ejekan
2	@tanduk_2.2	Video hoax kemudian hapus akun
3	@karambiaaa0	Akun asli
4	@muhammadromi_0.1	Target pesan

Setiap akun berbeda fungsi dan skenario dalam melakukan kejahatannya dalam satu telepon pintar, berikut penjelasannya:

a. Akun pertama dengan username @kell_1.3 sebagai pengunggah postingan video SARA dan melakukan pelecehan secara verbatim mengirim pesan ke akun @muhammadromi_0.1 lalu menghapusnya.
b. Akun kedua dengan username @tanduk_2.2 melakukan unggahan video hoax kemudian menghapus akunnya.
c. Akun keempat dengan username @karambiaaa0 akun terakhir sebagai akun asli dari pelaku.
d. Akun kelima dengan username @muhammadromi_0.1 merupakan akun target untuk kejahatan.

4.4 Skenario dan Simulasi Kasus

Tahap ini membangun sebuah skenario dan simulasi kasus agar dapat berjalan sesuai arahan penyelesaian masalah kasus, kondisi telepon pintar ditemukan dalam keadaan hidup dan sebelumnya sudah pernah di *root* oleh pelaku, diketahui saat melakukan ekstraksi berkas dari telepon pintar, proses ekstraksi dilakukan hanya khusus pada aplikasi TikTok versi 16.6.4. saat melakukan akuisisi telepon pintar menunjukkan informasi *unlocked* di proses *booting*, seperti pada gambar 4.2 dan gambar 4.3 sebagai simulasi kasus.



Gambar 4.2 Skenario Kasus

Skenario dan simulasi kasusnya pada telepon pintar Android dengan perangkat Xiaomi Redmi 5. Akun yang masuk pertama adalah *username* @tanduk_2.2, akun ini sedikit unik karena melakukan kegiatan unggahan video hoax. Video tersebut diunggah dengan konten memberikan informasi palsu, kemudian pelaku menghapus akunnya.

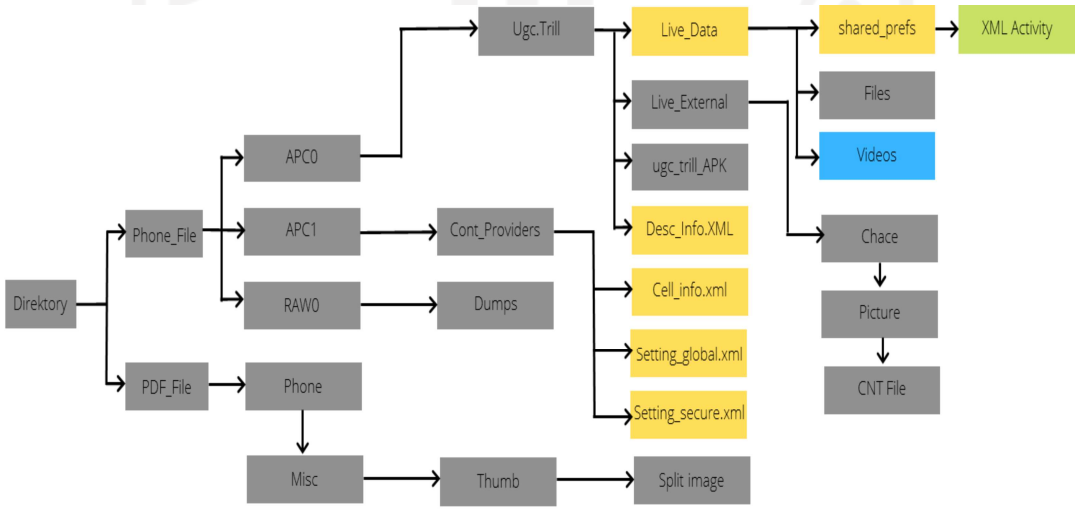
Setelah akun @tanduk_2.2 dihapus lalu akun dengan *username* @karambiaaa0 masuk, kegiatan-kegian yang dilakukan oleh akun tersebut hanya sebatas menjelajah beranda. Namun, akun tersebut tidak terdapat indikasi aktivitas kejahatan apapun hanya sebagai akun orisinal pelaku, setelah melakukan kegiatannya, akun @karambiaaa0 keluar

dan masuk disusul oleh akun *username* @kell_1.3 dengan melakukan beberapa kegiatan yang terinci.

Username @kell_1.3 melakukan kegiatan pada aplikasi TikTok seperti menggunakan fitur pencarian dengan beberapa kata kunci Agama, SARA, Jack_0.4, tanduk_2.2, karambiaaa0, khoax dan muhammadromi_0.1. Setelah melakukan pencarian kemudian lanjut dengan melihat video pada beranda lalu membuat video SARA dengan konten menjelekkan sebuah agama dan mengunggahnya. Setelah melakukan kegiatan-kegiatan pencarian, jelajah beranda dan mengunggah video tibalah pada kegiatan inti yaitu mengirim pesan. Pesan yang dikirim kepada akun @muhammadromi_0.1 dengan pelecehan secara verbatim, setelah terkonfirmasi terkirim diakun @kell_1.3 kemudian pada perangkat yang dipakai pelaku pesan tersebut dihapus dengan maksud menghilangkan jejak.

4.5 Lokasi Berkas

Lokasi map pada direktori adalah kumpulan dari semua yang dipakai untuk analisis, hasil ekstrak dari telepon pintar ada tiga berkas pertama, berkas terpenting adalah *phone file* dan pdf *file.* Setiap berkas memiliki karakter berbeda. Karakternya berupa data yang disimpan, misalnya berkas *phone file* digunakan hampir seutuhnya artefak kegiatan di aplikasi TikTok terutama di berkas ugc trill. Tetapi, beberapa berkas XML berada di luarnya seperti *cell* info adalah sumber informasi dari sinyal yang digunakan saat tersambung internet.



Gambar 4.3 Lokasi Berkas XML

Berkas pdf *file* adalah potongan-potongan gambar dari video yang telah diunggah di aplikasi TikTok, gambar-gambar tersebut juga termasuk dari potongan efek yang digunakan

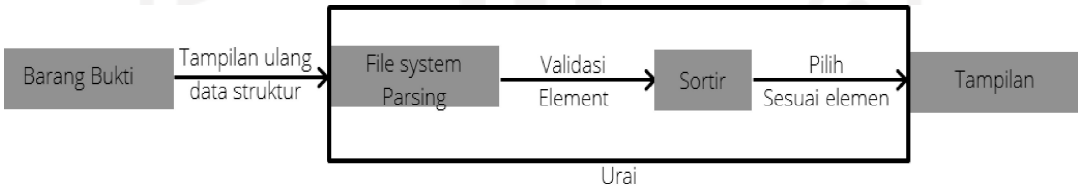
dalam video. Karakter semua gambar memiliki urutan dari Nama seperti img_7216, img_7217 dan seterusnya, ekstensi dalam kompres potongan gambar menggunakan png.

4.6 Analisis menggunakan DFXML

DFXML menyediakan cara untuk proses forensik umum misalnya hashing dan kriptografi. Forensik pada direktori seperti lokasi file pada hard drive juga pada bagian metadata Nama berkas dan *timestamp*. Berkas DFXML dibuat untuk setiap komponen umum XML dengan total lebih dari 800 baris, memiliki 72 elemen yang diperlukan dalam analisis. Elemen yang digunakan tidak semua pada berkas XML, elemen dapat menyesuaikan dengan kebutuhan dari metadata XML yang diproses.

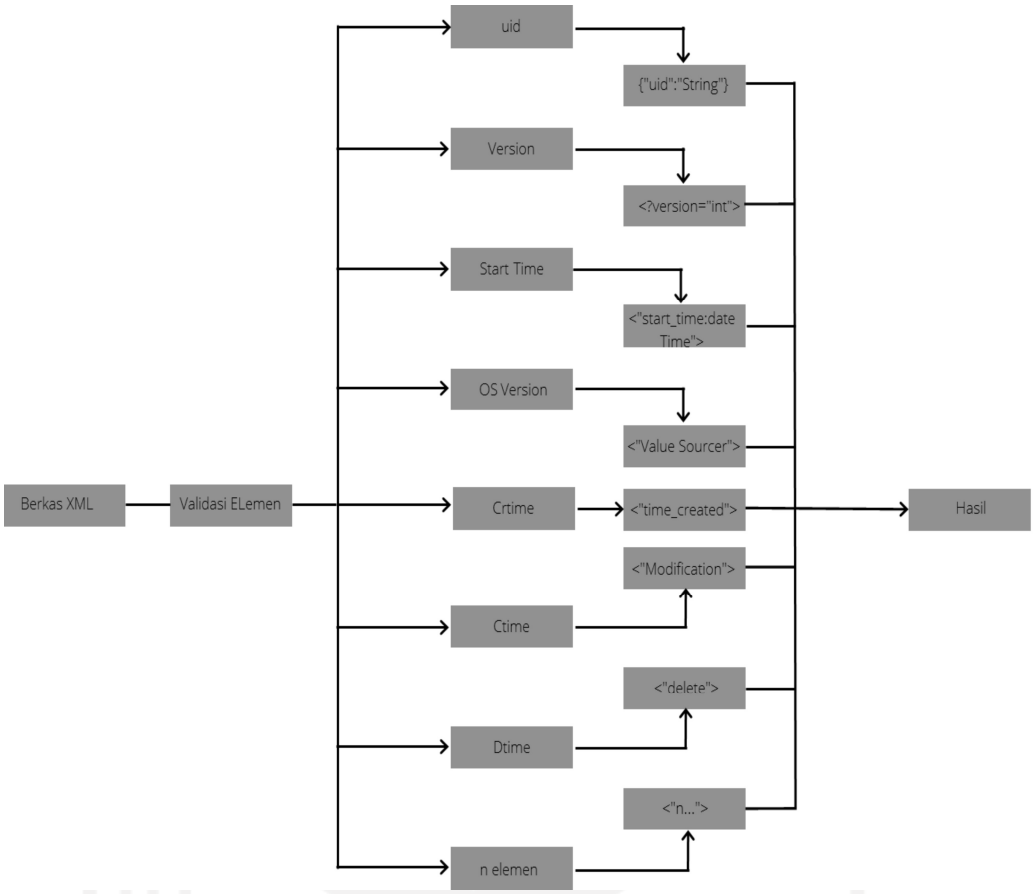
DFXML menyimpan output yang dapat memberikan informasi pengambilan dan representasi metadata sistem file untuk memastikan asal, keaslian, dan integritas media penyimpanan. Sebuah manifes yang cukup untuk memberlakukan navigasi penyimpanan penuh dan ekstraksi file tanpa perlu mengurai ulang struktur di disk setelah XML dibuat.

Penelitian ini menggunakan 9 elemen lebih dengan menyesuaikan kebutuhan pada data XML. Elemen terpenting adalah UID, karena mengikut dengan Satu akun yang terdapat pada telepon pintar untuk membedakan setiap perilakunya di aplikasi. Secara umum, alur kerja DFXML penelitian ini menguraikan struktur metadata untuk di serialisasikan kedalam pohon XML dengan mengambil metadata berkas penting saja.



Gambar 4.4 Metode Proses Uraian Berkas XML

Hal terpenting dalam tahapan pada gambar ialah di uraian sistem file, tahapan tersebut dilakukan untuk melihat isi data untuk disesuaikan dengan elemen yang dibutuhkan. Validasi elemen berperan penting karena tidak semua elemen pada DFXML dapat diterapkan pada berkas XML TikTok seperti elemen “mode” artinya mode berkas sedang dibuka. Berikut gambar tentang rincian Validasi elemen.



Gambar 4.5 Detail Uraian validasi Berkas XML

Validasi elemen dibutuhkan saat XML diuraikan. Elemen digunakan sesuai keperluan datanya, elemen dicocokkan dengan data di dalam XML. Apabila data sesuai dengan standar elemen dari NIST maka dapat dilanjutkan untuk dianalisis.

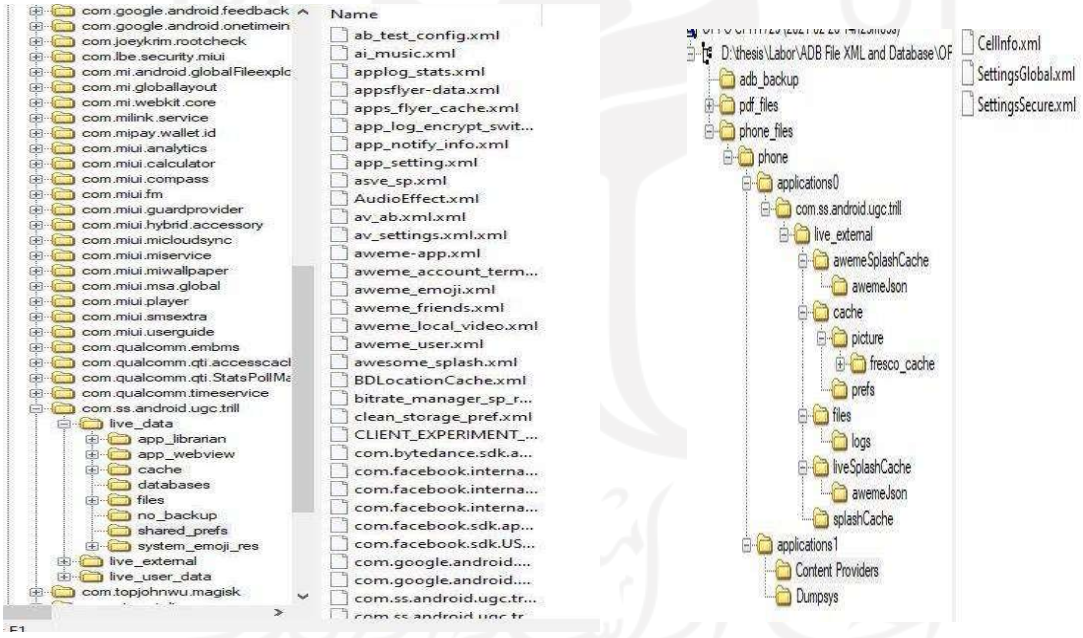
Aplikasi TikTok versi lawas dan terbaru memiliki perbedaan yang signifikan pada peningkatan jumlah berkas XML. Setiap pembaruan versi, beberapa berkas XML masih memiliki nama yang sama seperti aweme_user.xml berkas ini menyimpan data tentang pengguna TikTok dan apakah akun TikTok ditautkan ke Facebook, Twitter, Weibo, Youtube atau Instagram, jumlah pengikut, teman, dan akun yang diikuti. Selanjutnya berkas search.xml berisi informasi tentang riwayat pencarian yang dilakukan oleh pengguna.

Setiap aplikasi pada android memiliki jumlah sistem berkas metadata yang berbeda, bahkan antara aplikasi akan berbeda jika sudah berubah versi. Penelitian (Hoang Khoa et al., 2020), berkas XML pada aplikasi TikTok versi 8.9.4 ditemukan sebanyak 103 buah. Penelitian (Domingues et al., 2020), menemukan sebanyak 104 berkas XML pada aplikasi

TikTok versi 15.1.0. Setiap berkas XML yang ditemukan memiliki petunjuk aktivitas dari pengguna aplikasi.

Berkas XML aplikasi TikTok yang digunakan pada penelitian ini adalah versi 16.6.4. memiliki lebih dari 108 buah informasi potensial, seperti waktu aplikasi pertama kali dibuka, waktu instalasi aplikasi, aplikasi terakhir diperbaharui, alamat MAC SSID yang digunakan, riwayat pencarian dan lain-lain. Semua berkas XML terletak di area aplikasi pencadangan pada direktori com.ss.android.ugc.trill yang membutuhkan akses root pada telepon pintar. Berbeda dengan akses tanpa root hanya memiliki sedikit informasi diantaranya, Waktu pertama instal aplikasi, Waktu terakhir perbaharui aplikasi, Versi aplikasi, Sertifikat penggunaan aplikasi, Hak permisi pada android. Semua tersimpan pada direktori com.ss.android.ugc.trill\live_external.

Gambar 4.6 berikut mencantumkan spesifikasi perbedaan berkas XML antara telepon pintar yang sudah di root dan tanpa root.



A B

Gambar 4.6 A. Berkas XML Kondisi Root dan B. Berkas XML Kondisi Tanpa Root

Direktori aplikasi TikTok biasanya memiliki nama paket seperti com.ss.android.ugc.trill, semua informasi mulai dari database, *user* sampai dengan video unggahan berada di dalamnya, dilihat dari jumlah konten yang dimiliki oleh direktori ini

adalah 2,755 File dan 745 Folder dengan ukuran 204 MB. General informasi seperti pertama kali aplikasi dibuka, waktu install aplikasi, aplikasi terakhir di update sampai dengan daerah saat menggunakannya berada pada direktori *shared_prefs.* Semua konten pada direktori *shared_prefs* memiliki jumlah 107 berkas berekstensi XML.

4.6.1 Komponen Tentang Aplikasi TikTok

Komponen tentang aplikasi TikTok dapat dilihat pada direktori com.ss.android.ugc.trill, dengan Nama berkas "*description.info*" berukuran 4 KB, tipe berkasnya adalah "*XML Document"*. Informasi tambahan dapat diperoleh dari direktori com.ss.android.ugc.trill\live_data\shared_prefs nama berkas "*custom_channels.xml*". Beberapa informasi yang dapat diperoleh dari "*description.info.xml*"seperti *Application Size* 95.8 MB*, APK Verification Successful Yes, APK Verifications Schema 2, First Installed* 2021-02-19 14:36:05 (UTC+7) dan *Last Update* 2021-02-19 14:36:05 (UTC+7). Gambar 4.7 struktur APXML *description.info.xml*

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Appinfo type="Android">
<Name sourceValue="nonLocalizedLabel">TikTok</Name>
<Package sourceValue="packageName">com.ss.android.ugc.trill</Package>
<Version sourceValue="versionName">16.6.4</Version>
<AndroidValue sourceValue="versionCode">160604</AndroidValue>
<AndroidValue sourceValue="installLocation">/data/app/com.ss.android.ugc.trill-
XIvUQzj2XjZaB6g4SibbXg==/base.apk</AndroidValue>
<AndroidValue sourceValue="flags">953695812</AndroidValue>
<AndroidValue sourceValue="packageSize">95208458</AndroidValue>
<AppSize sourceValue="codeSize">0</AppSize>
<DataSize sourceValue="dataSize">0</DataSize>
<CacheSize sourceValue="cacheSize">0</CacheSize>
<AndroidValue sourceValue="derivedApplicationType">Regular Application</AndroidValue>
<AndroidValue sourceValue="firstInstallTime">20210219T073605Z</AndroidValue>
<AndroidValue sourceValue="lastUpdateTime">20210219T073605Z</AndroidValue>
<AppDataPath>/data/data/com.ss.android.ugc.trill</AppDataPath>
<AndroidValue
sourceValue="installerPackageName">com.google.android.packageinstaller</AndroidValue>
</Appinfo>
```

Gambar 4.7 Struktur APXML Tentang Aplikasi TikTok

Struktur APXML (Application Profile XML) pada gambar 4.7 memiliki metadata yang elemennya dapat mendokumentasikan. Elemen metadata mendokumentasikan informasi tambahan tentang profil aplikasi termasuk nama dan versi aplikasi menggunakan Appinfo hanya dapat diinstal di Android dengan *Label* TikTok, Sumber Nilai Paket com.ss.android.ugc.trill, *Version* 16.6.4, *Installed by* com.google.android.packageinstaller. Berkas XML tentang informasi versi aplikasi TikTok dapat juga disimpulkan dari berkas version. Gambar 4.8 Struktur APXML *version.xml*

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
-<map>
<string name="app_version">16.6.4</string>
</map>
```

Gambar 4.8 Struktur APXML *version.xml*

Informasi untuk sumber saluran aplikasi dipasang dapat dilihat pada Gambar 4.9 Struktur APXML *custom_channels.xml*

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
-<map>
<string
name="app_install_info">{"app_channel":"googleplay","apk_create_time":1613720149,"system
_create_time":1230739200,"has_send_app_info":true}</string>
</map>
```

Gambar 4.9 Struktur APXML *custom_channels.xml*

Informasi aplikasi yang diinstall memiliki saluran “googleplay”, waktu pembuatan aplikasi “1613720149” dan waktu pembuatan di sistem “1230739200”. Perangkat menggunakan WI-FI untuk mengakses jaringan agar dapat menjalankan aplikasi TikTok. Gambar 4.10 Informasi trafik jaringan.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
-<map>
<long value="1613987702553" name="collect_traffic_time"/>
<long value="0" name="wifi_traffic"/>
<string name="net_type">WIFI</string>
<int value="1" name="traffic_upload_switch"/>
<long value="0" name="mobile_traffic"/>
<long value="490216" name="last_total_traffic"/>
```

```
<long value="1613987702553" name="timestamp"/>
</map>
```

Gambar 4.10 Struktur XML informasi trafik jaringan.

Tampilan kesimpulan informasi yang didapat dari struktur APXML Tentang Aplikasi TikTok tersebut seperti pada tabel 4.4.

Tabel 4.4 Struktur APXML Tentang Aplikasi TikTok

No	Nama	Keterangan
1	Label	TikTok
2	Package	com.ss.android.ugc.trill
3	Version	16.6.4
4	Application Type	User Application
5	Sideloaded Application	Yes
6	Installed by	com.google.android.packageinstaller
7	Application Size	90.8 MB
8	Cache Size	0 B
9	APK File Extracted	Yes
0	APK Verification Successful	Yes
10	APK Verification Scheme	2
11	First Installed	2021-02-19 14:36:05 (UTC+7)
12	Last Updated	2021-02-19 14:36:05 (UTC+7)

Informasi berikutnya ialah tipe aplikasi hanya untuk tingkat pengguna saja, *sideloaded application* adalah keterangan untuk persetujuan instalasi menggunakan aplikasi yang tidak diunduh pada *playstore. APP File Extracted* menandakan bahwa saat pemasangan aplikasi akan diekstrak dari paket untuk dapat digunakan.

4.6.2 Komponen Masuk

Masuk aplikasi TikTok akan meninggalkan jejak mulai dari metode yang digunakan, email, kadaluarsa akun, waktu masuk, UID yang digunakan serta avatar URL. Gambar 0.0 Struktur XML masuk aplikasi TikTok.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>-<map><string
name="latest_login_info">[{"name":"tanduk222222@gmail.com","commonUserInfo":{"avatarUrl":"https
://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp?x-
expires\u003d1613808000\u0026x-
signature\u003dXopf2O0xFqJDb3RLUwvmOywUBWo%3D","secUid":"MS4wLjABAAAAWNieRQx9x
-pXSz5LBq2niReoXVRgL6X4ooWGd6Vk-
```

q2Ul68F9C7D__D24YSyhJ_p","userName":"tanduk_2.2"},"expires":"Mar 21, 2021 3:04:27 PM","lastActiveTime":1613721867401,"loginMethodName":"EMAIL_PASS","loginTime":1613721513854,"uid":"6930553924097590274"},{"name":"jack0000000004@gmail.com","commonUserInfo":{"avatarUrl":"https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp?x-expires\u003d1613808000\u0026x-signature\u003dXopf2O0xFqJDb3RLUwvmOywUBWo%3D","secUid":"MS4wLjABAAAAxAXFxpQE-5SprVeHWJ5IGnZz6X7X0ca8AOZV9ppfMUA0-BInDcet7O5FxQWf3vF4","userName":"jack_0.4"},"expires":"Mar 21, 2021 2:51:39 PM","lastActiveTime":-1,"loginMethodName":"EMAIL_PASS","loginTime":1613721099641,"uid":"6930552960570000386"},{"name":"kell0000011@gmail.com","commonUserInfo":{"avatarUrl":"https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp?x-expires\u003d1613808000\u0026x-signature\u003dXopf2O0xFqJDb3RLUwvmOywUBWo%3D","secUid":"MS4wLjABAAAAKrnEpz3gQIsda93DwsYtMpaltqZCVfpmom8z-PaLswRt2nwHNtlYQgCvQ_6g3Ve3","userName":"Kell_1.3"},"expires":"Mar 21, 2021 2:38:47 PM","lastActiveTime":-1,"loginMethodName":"EMAIL_PASS","loginTime":1613720327000,"uid":"6930551655360414721"}]</string></map>

Gambar 4.11 Struktur XML masuk aplikasi TikTok

Informasi dari Gambar 4.11 memiliki 3 akun yang melakukan masuk aplikasi, sebagai berikut:

1. Akun @tanduk_2.2

   Akun @tanduk_2.2 melakukan masuk menggunakan metode Email dan Password "EMAIL_PASS", email "tanduk222222@gmail.com", kadaluarsa akun "Mar 21, 2021 3:04:27 PM", waktu masuk "1613721513854" dan UID yang digunakan "6930553924097590274" serta avatar URL https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp.
2. Akun @jack_0.4

   Akun @jack_0.4 melakukan masuk menggunakan metode Email dan Password "EMAIL_PASS", email "jack0000000004@gmail.com", kadaluarsa akun "Mar 21, 2021 2:51:39 PM", waktu masuk "1613721099641" dan UID yang digunakan "6930552960570000386" serta avatar URL https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp.
3. Akun @kell_1.3

Akun @kell_1.3 melakukan masuk menggunakan metode Email dan Password "EMAIL_PASS", email "kell0000011@gmail.com", kadaluarsa akun "Mar 21, 2021 2:38:47 PM", waktu masuk "1613720327000" dan UID yang digunakan "6930551655360414721" serta avatar URL https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp.

4.6.3 Komponen Fungsional Akun

Penelitian ini menggunakan 4 akun dalam melakukan eksperimen dengan Tiga akun kejahatan @kell_1.3, @tanduk_2.2, Satu akun asli @karambiaaa0 dan Satu akun target @muhammadromi_0.1. Analisis dilakukan fokus terhadap Tiga akun pertama dalam mengambil barang bukti. Komponen informasi utama dalam Tiga akun yang digunakan adalah Nama akun, Nama pendek, avatar URL, jenis kelamin, uID, mode.

Informasi dari pengguna akun berada pada direktori *aweme_user.xml* nama paketnya com.ss.android.ugc.trill di sub direktori *shared_pref.* sebagai contoh pada gambar 4.12 informasi dari akun @karambiaaa0 yang telah digunakan dan tersimpan pada *aweme_user.xml* dengan keterangan nama "6896333489403724802", nama pendek "karambia aa", unique id "karambiaaa0, mode anak "tidak" dengan lambang "0", avatar URL https://p16-sign-sg.tiktokcdn.com/aweme/100x100/tiktok-obj/1683676134080514.webp.

```
<string
name="6896333489403724802_significant_user_info">{"uid":"6896333489403724802","short_
id":"0","unique_id":"karambiaaa0","nickname":"karambia aa","avatar_url":"https://p16-sign-
sg.tiktokcdn.com/aweme/100x100/tiktok-obj/1683676134080514.webp?x-
expires\u003d1613808000\u0026x-
signature\u003dF%2FGeSW6ybEsY4xWFfRpPO%2FpTrDA%3D"}</string>
</string>
```

Gambar 4.12 Informasi Akun @karambiaaa0

Selanjut tahapan analisis pada 2 akun yang digunakan untuk kejahatan sebagai berikut:

1. Akun @kell_1.3

   Akun @kell_1.3 adalah yang melakukan unggahan video SARA. Informasi yang dapat diambil dari berkas *aweme_user.xml* cukup lengkap pada bagian keterangan akunnya, seperti UID "6930551655360414721", short_id "0", unique_id "kell_1.3", nama pendek "Kell_1.3", avatar_url i"https://p16-sign-

sg.tiktokcdn.com/aweme/100x100/tiktok-obj/1683676134080514.webp". Aktivitas masuk terlihat delapan kali pada aplikasi untuk semua akun saat sedang beroperasi di akun @kell_1.3, tercatat dengan nomor masuk 1594805258216454 kemudian masuk kembali di alamat avatar yang sama "https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_1080x1080.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dN6F6L4RMeVUudzGgMVt5Ggst54U%3D" sebanyak Tujuh kali.

<string name="**6930551655360414721_significant_user_info**">{"uid":"6930551655360414721","short_id":"0","unique_id":"kell_1.3","nickname":"Kell_1.3","avatar_url":"https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp?x-expires\u003d1613808000\u0026x-signature\u003dXopf2O0xFqJDb3RLUwvmOywUBWo%3D"}</string><string name="**6930551655360414721_aweme_user_info**">{"accept_private_policy":false,"account_region":"","account_type":0,"allowStatus":0,"authority_status":0,"avatar_larger":{"height":0,"data_size":0,"uri":"musically-maliva-obj/1594805258216454","url_list":["https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_1080x1080.webp?x-expires\u003d1613808000\u0026x-signature\u003dre3HHNF98wm%2FUaZHqr9hxiZmlIQ%3D","https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_1080x1080.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dN6F6L4RMeVUudzGgMVt5Ggst54U%3D"],"width":0},"avatar_medium":{"height":0,"data_size":0,"uri":"musically-maliva-obj/1594805258216454","url_list":["https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_720x720.webp?x-expires\u003d1613808000\u0026x-signature\u003djxf5GmoA8E25TbYGHNrbb2MI5pA%3D","https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_720x720.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dKX0OLuMzf5w6qu6GspVWDTvI27M%3D"],"width":0},"avatar_thumb":{"height":0,"data_size":0,"uri":"musically-maliva-obj/1594805258216454","url_list":["https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.webp?x-expires\u003d1613808000\u0026x-signature\u003dXopf2O0xFqJDb3RLUwvmOywUBWo%3D","https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dkSsDaS5l4lzQhQjofvr1fk%2Bi7ds%3D"],"width":0},"avatar_update_reminder":false,"video_icon":{"height":0,"data_size":0,"uri":"","url_list":[],"width":0},"aweme_count":1,"aweme_hotsoon_auth":0,"aweme_hotsoon_auth_relation":0,"bind_phone":"","bio_permission":{"enable_email":false,"enable_location":false,"enable_phone":false,"enable_url":false},"birthday_hide_level":0,"can_modify_school_info":false,"can_set_geofencing":false,"cancel_type":0,"category":"","collect_count":0,"comment_filter_status":0,"comment_setting":0,"commerce_permissions":{"e_homepage_tab_management":-1,"elite_login":-1,"enterprise":-1,"head_image":-1,"star_atlas_order":-1,"top_item":-

1},"commerce_user_info":{"ad_authorization":false,"ad_influencer_type":0,"has_ads_entry":false,"is_ad_partner":false,"is_auction_ad_influencer":false,"show_star_atlas_cooperation":false,"star_atlas":0},"commerce_user_level":0,"constellation":0,"cover_url":[{"height":0,"data_size":0,"uri":"tiktok-obj/1613727517271041","url_list":["https://p16-sg.tiktokcdn.com/obj/tiktok-obj/1613727517271041","https://p53-sg.tiktokcdn.com/obj/tiktok-obj/1613727517271041"],"width":0}],"custom_verify":"","display_wvalantine_activity_entry":false,"dongtai_count":0,"dou_plus_share_location":0,"download_setting":0,"duet_setting":0,"education":0,"email":"k***1@gmail.com","enterprise_verify_reason":"","mplatform_followers_count":0,"favoriting_count":0,"fb_expire_time":0,"follow_status":0,"follower_count":0,"follower_status":0,"following_count":2,"force_private_account":false,"friend_count":0,"gender":0,"google_account":"","has_email":true,"has_facebook_token":false,"has_activity_medal":false,"has_orders":false,"has_story":false,"has_twitter_token":false,"has_youtube_token":false,"hide_location":false,"hide_following_follower_list":0,"hide_search":false,"hide_shoot_button":false,"ins_id":"","is_activity_user":false,"is_ad_fake":false,"is_binded_weibo":false,"is_block":false,"is_blocked":false,"content_language_already_popup":false,"has_insights":false,"is_discipline_member":false,"is_effect_artist":false,"is_email_verified":true,"is_flowcard_member":false,"is_minor":false,"isNewRecommend":false,"douplus_old_user":false,"is_phone_binded":false,"is_pro_account":false,"is_star":false,"sync_to_toutiao":0,"is_verified\u0027":false,"iso_country_code":"","latest_order_time":0,"live_agreement":0,"live_commerce":false,"login_platform":0,"mAtType":0,"is_gov_media_vip":false,"music_compliance_account":0,"need_addr_card":false,"need_recommend":false,"neiguang_shield":0,"nickname":"Kell_1.3","nickname_update_reminder":false,"normal_top_comment_permission":0,"notify_private_account":0,"original_musician":{"digg_count":0,"music_count":0,"music_used_count":0},"post_default_download_setting":true,"prevent_download":false,"private_aweme_count":0,"pro_account_tcm_red_dot":false,"profile_completion":0.0,"profile_pv":0,"recommend_score":0.0,"registerStatus":0,"register_time":1613650106,"forward_count":0,"room_id":0,"school_visible":0,"school_type":0,"sec_uid":"MS4wLjABAAAAKrnEpz3gQIsda93DwsYtMpaltqZCVfpmom8z-PaLswRt2nwHNtlYQgCvQ_6g3Ve3","secret":false,"share_info":{"bool_persist":1,"share_image_url":{"height":0,"data_size":0,"uri":"musically-maliva-obj/1594805258216454","url_list":["https://p16-sign-sg.tiktokcdn.com/obj/musically-maliva-obj/1594805258216454?x-expires\u003d1613743200\u0026x-signature\u003dZbtMKZEhlz%2BIlpbPBo1cCBa%2BHEk%3D"],"width":0},"share_desc":"Lihat Kell_1.3! #TikTok","share_title":"Bergabung dengan TikTok dan lihat yang saya kerjakan!","share_title_myself":"Aplikasi TikTok ini sangat asyik! Ikuti saya @Kell_1.3 di TikTok dan lihat video saya!","share_title_other":"Pengguna TikTok ini keren sekali. Ikuti @Kell_1.3 di TikTok dan lihat video yang hebat itu!","share_url":"https://t.tiktok.com/i18n/share/user/6930551655360414721/?_d\u003ddh56j90e002kih\u0026language\u003did\u0026sec_uid\u003dMS4wLjABAAAAKrnEpz3gQIsda93DwsYtMpaltqZCVfpmom8z-PaLswRt2nwHNtlYQgCvQ_6g3Ve3\u0026share_author_id\u003d6930551655360414721\u0026u_code\u003ddh5iba3j57c7mi","share_weibo_desc":"TikTok: Membuat Setiap Detik Berharga"},"shield_comment_notice":0,"shield_digg_notice":0,"shield_follow_notice":0,"short_id":"0","should_write_impr":false,"show_artist_playlist":0,"show_favorite_list":false,"show_gender_strategy":0,"sh

ow_image_bubble":false,"message_chat_entry":true,"show_user_ban_dialog":false,"signature":"","star_billboard_rank":0,"star_use_new_download":false,"story_count":0,"story_open":false,"tab_settings":{"hide_like_tab":false,"private_tab":{"private_tab_style":2}},"profile_tab_type":0,"total_favorited":0,"tw_expire_time":0,"twitter_id":"","twitter_name":"","uid":"6930551655360414721","unique_id":"kell_1.3","unique_id_modify_time":0,"user_canceled":false,"user_mode":1,"user_period":0,"user_rate":1,"user_story_count":0,"verification_badge_type":0,"verification_type":0,"verify_info":"","realname_verify_status":0,"video_cover":{},"watch_status":0,"with_commerce_enterprise_tab_entry":false,"with_commerce_entry":false,"with_commerce_newbie_task":false,"with_dou_entry":true,"with_douplus_entry":false,"with_fusion_shop_entry":false,"with_item_commerce_entry":false,"with_luban_entry":false,"with_new_goods":false,"with_shop_entry":false,"with_star_atlas_entry":false,"wx_tag":0,"xmas_unlock_count":0,"youtube_last_refresh_time":0,"youtube_refresh_token":"","youtube_channel_id":"","youtube_channel_title":"","youtube_expire_time":0}</string>

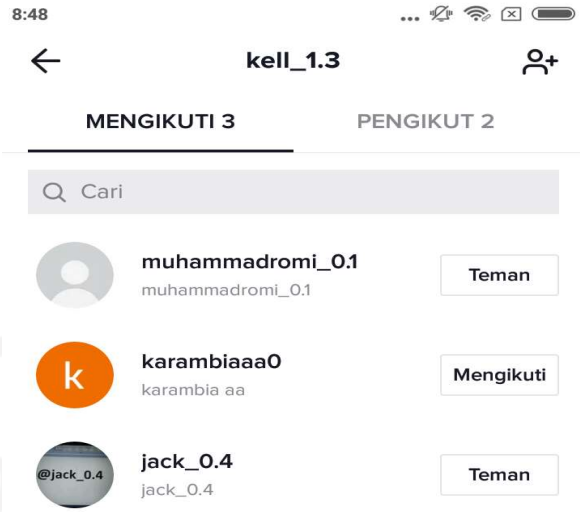
Gambar 4.13 Informasi Akun @kell_1.3

2. Akun @Tanduk_2.2

   Akun @Tanduk_2.2 mengunggah sebuah video hoax kemudian menghapus akunnya, jejak yang ditinggalkan pada artefak digital tidak ditemukan sama sekali pada bagian informasi pengguna di berkas *aweme_user.xml*. Namun meninggal jejak lain seperti masuk aplikasi, video yang diunggah, efek yang digunakan dan musik yang mengiringi video.

4.6.4 Komponen Fungsional Teman

Cara kerja fungsional teman pada aplikasi TikTok adalah dengan saling mengikuti maka akan masuk ke dalam daftar teman. Kemudian, antara teman akan dapat saling bertukar pesan. Teman pada akun @kell_1.3 ialah Muhammadromi_0.1 dan jack_0.4, seperti pada gambar 4.14 daftar pertemanan.



Gambar 4.14 Daftar Pertemanan

Pembuktian jumlah teman dari akun @kell_1.3 dapat diperoleh dari *aweme_user.xml* pada baris **<string name="6930551655360414721_significant_user_info">**. Konten metadata xml pada gambar 4.15 informasi yang berkaitan dengan teman adalah pada bagian kode "following_count:2".

https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/1594805258216454~c5_100x100.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dkSsDaS5l4lzQhQjofvr1fk%2Bi7ds%3D"
":"","display_wvalantine_activity_entry":false,"dongtai_count":0,"dou_plus_share_location":0,"download_setting":0,"duet_setting":0,"education":0,"email":"k***1@gmail.com","enterprise_verify_reason":"","mplatform_followers_count":0,"favoriting_count":0,"fb_expire_time":0,"follow_status":0,"follower_count":0,"follower_status":0,**"following_count":2**,"force_private_account":false,"friend_count":0,"gender":0,"google_account":"","has_email":true,"has_facebook_token":false,"has_activity_medal":false,"has_orders":false,"has_story":false,"has_twitter_token":false,"has_youtube_token":false,"hide_location":false,"hide_following_follower_list":0,"hide_search":false,"hide_shoot_button":false,"ins_id":"","is_activity_user":false,"is_ad_fake":false,"is_binded_weibo":false,"is_block":false,"is_blocked":false,"content_language_already_popup":false,"has_insights":false,"is_discipline_member":false,"is_effect_artist":false,"is_email_verified":true,"is_flowcard_member":false,"is_minor":false,"isNewRecommend":false,"douplus_old_user":false,"is_phone_binded":false,"is_pro_account":false,"is_star":false,"sync_to_toutiao":0,"is_verified\u0027":false,"iso_country_code":"","latest_order_time":0,"live_agreement":0,"live_commerce":false,"login_platform":0,"mAtType":0,"is_gov_media_vip":false,"music_compliance_account":0,"need_addr_card":false,"need_recommend":false,"neiguang_shield":0,"nickname":"Kell_1.3","nickname_update_reminder":false,"normal_top_comment_permission":0,"notify_private_account":0,"original_musician":{"digg_count":0,"music_count":0,"music_used_count":0},"post_default_download_setting":true,"prevent_download":false,"private_aweme_count":0,"pro_account_tcm_red_dot":false,"profile_completion":0.0,"profile_pv":0,"recomme

nd_score":0.0,"registerStatus":0,"register_time":1613650106,"forward_count":0,"room_id":0,"school_visible":0,"school_type":0,"sec_uid":"MS4wLjABAAAAKrnEpz3gQIsda93DwsYtMpaltqZCVfpmom8z-PaLswRt2nwHNtlYQgCvQ_6g3Ve3","secret":false,"share_info":{"bool_persist":1,"share_image_url":{"height":0,"data_size":0,"uri":"musically-maliva-

Gambar 4.15 Informasi Jumlah Teman

Avatar URl yang tercatat dalam metadata adalah https://p16-sign-sg.tiktokcdn.com/musically- maliva-obj/1594805258216454~c5_100x100.jpeg?x-expires\u003d1613808000\u0026x-signature\u003dkSsDaS5l4lzQhQjofvr1fk%2Bi7ds%3D dimiliki oleh akun @jack_0.4 salah satu teman dari akun @kell_1.3.

4.6.5 Komponen Direktori Video

Setiap video yang dibuat, diunggah kemudian akan secara langsung tersimpan. Artefak tersebut, dapat dilihat pada *aweme_local_video.xml*, memberikan informasi yang cukup lengkap mulai dari ID akun yang membuat video, lokasi direktori video tersimpan, nama berkas, waktu pembuatan video, durasi dan jenis standar video. Gambar 4.16. Informasi direktori video.

<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<map><string name="**extra_data**">{"6930877942188788994":{"local_path":"/data/user/0/com.ss.android.ugc.trill/files/synthetise_2021-02-19-144205227-concat-v","author_id":"6930551655360414721","**create_time":185068285,"**duration":8006.0,"is_h265":false,"m_vr":false,"ratio_uri":"v07025e80000c0nmpcbrgkfme10fb8o0_h264_540p_3922628","source_id":"6930877942188788994","height":960,"data_size":0,"uri":"v07025e80000c0nmpcbrgkfme10fb8o0_h264_540p_3922628","width":544},"6930882230294220033":{"local_path":"/data/user/0/com.ss.android.ugc.trill/files/synthetise_2021-02-19-150002736-concat-v","author_id":"6930553924097590274","create_time":186066687,"duration":10534.0,"is_h265":false,"m_vr":false,"source_id":"6930882230294220033","height":960,"data_size":0,"uri":"v070258e0000c0nn14f2slelrukj5ob0_h264_540p_3888039","width":544}}</string></map>

Gambar 4.16. Informasi direktori video.

Akun yang melakukan unggahan video adalah “6930551655360414721”, video tersimpan pada direktori “com.ss.android.ugc.trill/files/” nama berkas “synthetise_2021-02-19-144205227-concat-v”, waktu pembuatan video “185068285”, jenis standar video bukan H264 dan memiliki durasi “80006.0”. akun selanjutnya “6930553924097590274”,

tersimpan pada direktori yang sama dengan nama berkas “synthetise_2021-02-19-150002736-concat-v”, waktu pembuatan “186066687” , durasi video “10534.0” dan Tidak mendukung standar H265.

4.6.6 Komponen Metadata Rekaman Video

Video yang diterbitkan, akan disimpan juga dalam bentuk metadata XML. Setiap metadata memberikan informasi yang banyak seperti *Audio bit rate, composition video resolution width, record video resolution width, effect version, record video resolution height* dan *user device.* Gambar 4.17 Struktur XML metadata rekaman video.


```
<?xml version="1.0" encoding="UTF-8" standalone="true"?> -<map>
<int value="10" name="shoot_mode"/>
<string name="filter_ids">232751</string>
<string name="reaction">null</string>
<string name="poi_context"/>
<string name="music_model"/>
<long value="15000" name="max_duration"/>
<string name="stitch_params">null</string>
<string
name="video_record_metadata">{"te_os":1,"te_edit_effect":0,"te_ve_version":"7.0.0.229","te_record_vid
eo_encode_mode":1,"te_composition_audio_bit_rate":128,"te_record_video_profile":"high","te_composit
ion_video_resolution_width":544,"te_record_video_resolution_width":544,"te_effect_version":"7.0.0_rel_
10_MT_202006171421_d357e092f4","te_record_video_resolution_height":960,"te_edit_hdr":0,"te_is_ree
ncode":0,"te_record_video_bit_rate":5000000,"te_composition_video_resolution_height":960,"te_edit_bri
ght_enhance":0,"te_composition_audio_samplerate":44100,"te_audio_effect":"","te_record_video_frame_
rate":-
1,"te_system":27,"te_record_video_encode_type":"h264","te_composition_audio_encode_type":"aac","te
_user_device":"Redmi 5A"}</string>
<int value="0" name="music_start"/>
<int value="0" name="record_mode"/>
<string name="segment_video"/>
<string name="duet_audio_path"/>
<int value="0" name="face_beauty"/>
<string name="mp4_path"/>
<string name="duet_video_path"/>
<string name="challenge"/>
<int value="0" name="hard_encode"/>
<string name="filter_labels">F1</string>
<string name="creation_id"/>
```

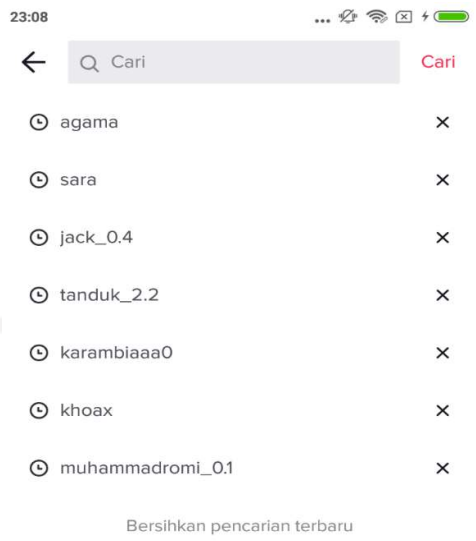
<string name="comment_video_moodel"/>
<string
name="shot_extract_frame">{"extractFramesDir":"/data/user/0/com.ss.android.ugc.trill/files/extract_shot/6fc360e6-8924-41b7-9fa2-1ba38ec7e3da","extractType":"extract_shot","frames":{"0":["/data/user/0/com.ss.android.ugc.trill/files/extract_shot/6fc360e6-8924-41b7-9fa2-1ba38ec7e3da/extract-frame-1613721607574.jpg","/data/user/0/com.ss.android.ugc.trill/files/extract_shot/6fc360e6-8924-41b7-9fa2-1ba38ec7e3da/extract-frame-1613721609575.jpg","/data/user/0/com.ss.android.ugc.trill/files/extract_shot/6fc360e6-8924-41b7-9fa2-1ba38ec7e3da/extract-frame-1613721611576.jpg","/data/user/0/com.ss.android.ugc.trill/files/extract_shot/6fc360e6-8924-41b7-9fa2-1ba38ec7e3da/extract-frame-1613721613579.jpg","/data/user/0/com.ss.android.ugc.trill/files/extract_shot/6fc360e6-8924-41b7-9fa2-1ba38ec7e3da/extract-frame-1613721615580.jpg","/data/user/0/com.ss.android.ugc.trill/files/extract_shot/6fc360e6-8924-41b7-9fa2-1ba38ec7e3da/extract-frame-1613721617582.jpg"]},"stickerFacesMap":{}}</string>
<string name="music_path"/>
</map>

Gambar 4.17 Struktur XML metadata rekaman video

Informasi struktur dari gambar 4.17 adalah composition audio bit rate “128”, composition video resolution width “544”, record video resolution width “544”, effect version “7.0.0_rel_10_MT_202006171421_d357e092f4”, record video resolution height “960”, user device “Redmi 5A” dan extract frames direktori “/data/user/0/com.ss.android.ugc.trill/files/extract_shot/6fc360e6-8924-41b7-9fa2-1ba38ec7e3da”.

4.6.7 Komponen Fungsional Pencarian

Fungsional pencarian adalah mencari dengan kata kunci akun atau judul video, bahkan pada saat pencarian akan disarankan beberapa video yang sedang tren. Pada gambar 4.10 aksi fungsional pencarian di aplikasi TikTok.



Gambar 4.18 Aksi fungsional pencarian di aplikasi TikTok

Berkas XML pencarian dapat ditemukan pada direktori *shared_prefs,* nama berkasnya adalah *search.xml* dengan ukuran 1 KB. Kode berkas XML pencarian seperti pada gambar 4.19 informasi kegiatan pencarian yang dilakukan pada aplikasi TikTok.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<map><string
name="recent_history">[{"keyword":"muhammadromi_0.1","int":0},{"keyword":"khoax","int":0},
{"keyword":"karambiaaa0","int":0},{"keyword":"tanduk_2.2","int":0},{"keyword":"jack_0.4","int":
0},{"keyword":"sara","int":0},{"keyword":"agama","int":0}]</string><string
name="place_holder">Cari</string></map>
```

Gambar 4.19 Informasi kegiatan pencarian yang pada aplikasi TikTok

Baris code name="**recent_history**" adalah semua kegiatan pencarian yang dilakukan. Pencarian memiliki tujuh kata kunci yaitu muhammadromi_0.1, khoax, karambiaaa0, tanduk_2.2, jack_0.4, Sara dan Agama.

4.7 Analisis Database

Analisis database penelitian ini adalah percakapan, video, localHashTag, downloader, ss_app_log, gecko_local_info dan web_offline_statistic.

4.7.1 Analisis Database Percakapan

Layaknya media sosial lain, TikTok juga dapat melakukan pertukaran pesan dengan syarat antara akun sudah saling mengikuti sehingga status dari "Mengikuti" menjadi "Teman". Apabila pesan sudah dikirimkan ke daftar teman, semua pesan akan tersimpan pada database. Gambar 4.20 teks pesan yang dikirimkan oleh akun @kell_1.3 ke akun @muhammadromi_0.1.

Gambar 4.20 Teks pesan

Lokasi DB pesan ada di direktori *live_data,* setiap DB pesan akan diawali dengan UID milik pengirim diikuti dengan bacaan _im berekstensi .db. Kasus ini UID kell_1.3 adalah "6930551655360414721", Nama berkasnya adalah "6930551655360414721_im.db". Gambar 4.21 bentuk XML pada bagian konten pesan yang dikirim.

{"type":0,"isDefault":false,"text":"**jelek Lo mirip banget aa monyet \ntolol bodoh eek kontol lo**","is_card":false,"mSendStartTime":1613722263921,"msgHint":"","aweType":700}

Gambar 4.21 Visual XML konten pesan

Pesan yang dikirim sebelumnya tersimpan di dalam database. Sebagai catatan dapat ditampilkan dalam bentuk XML, Kode unik "\n" menandakan pesan selanjutnya dalam kondisi baris baru "enter" pada saat penulisan kemudian dikirim ke target. Jadi konten sebenarnya adalah "jelek Lo mirip banget aa monyet tolol bodoh eek kontol lo". Pertukaran pesan antar akun dapat dilihat pada bagian tabel "participant" seperti pada gambar 4.22.

Table: participant

	user_id
	Filter
1	6896334472335590402
2	6930551655360414721

Gambar 4.22 Akun yang bertukar pesan

UID “6930551655360414721” dimiliki oleh akun kell_1.3 dan target pesannya memiliki UID “6896334472335590402” dengan nama akun muhammadromi_0.1.

4.7.2 Analisis Video

Artefak video dari aplikasi TikTok sangat berbeda antara versi 8.9.4 dengan versi 16.0.41 di penelitian ini. Pada versi 8.9.4 video yang dilihat oleh pengguna masih disimpan pada direktori applications0\com.ss.android.ugc.trill\live_data\databases\ nama berkasnya video.db, sebagai catatan apabila dapat diakses seperti pada gambar 4.23 informasi berisi catatan video yang dilihat pengguna.

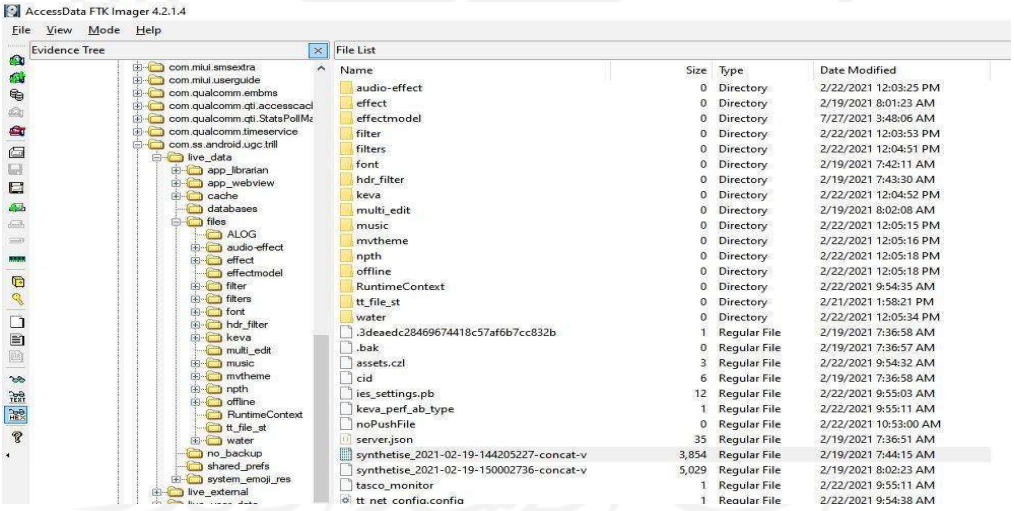
	_id	key	mime	contentLength	flag	extra
		Filter	Filter	Filter		Filter
1	1	A92814A4F888...	video/mp4	3255700	0	{"requestUrl":"http:\/\/v9.tiktokcdn.com\/ca
2	2	F180814E6F23...	video/mp4	3814189	0	{"requestUrl":"http:\/\/v9.tiktokcdn.com\/2
3	3	273358D46D7F...	video/mp4	1617565	0	{"requestUrl":"http:\/\/v9.tiktokcdn.com\/5
4	4	5DB006933FB4...	video/mp4	1285935	0	{"requestUrl":"http:\/\/v16.tiktokcdn.com\/
5	5	9676006ADDD...	video/mp4	913243	0	{"requestUrl":"http:\/\/v16.tiktokcdn.com\/
6	6	10497D24EC06...	video/mp4	1438301	0	{"requestUrl":"http:\/\/v16.tiktokcdn.com\/
7	7	410143235120...	video/mp4	1190241	0	{"requestUrl":"http:\/\/v16.tiktokcdn.com\/
8	8	02779B5FE802...	video/mp4	1515323	0	{"requestUrl":"http:\/\/v16.tiktokcdn.com\/
9	9	3C31B40EC0C2...	video/mp4	1908948	0	{"requestUrl":"http:\/\/v16.tiktokcdn.com\/
10	10	D6BA2A973B81...	video/mp4	377885	0	{"requestUrl":"http:\/\/v16.tiktokcdn.com\/

Gambar 4.23 informasi catatan video yang dilihat pengguna

Berbeda dengan TikTok versi 16.0.41 sama sekali tidak dapat ditemukan database video yang telah ditonton oleh pengguna, setelah melakukan penelusuran pada bagian direktori database, artefak database video yang dilihat oleh pengguna kemungkinan sudah tidak diberikan akses untuk dilihat.

Media pada TikTok yang dibuat dan disimpan memiliki 3 berkas terpisah, kode v berarti video, kode a berarti audio. Perpaduan antara video dan audio menjadi video akan bernama awalan mix. Selain dari penyimpanan dalam bentuk database, penelusuran pada penelitian ini ditemukan dalam bentuk berkas video dalam format type "*file*", Setiap video yang dibuat akan disimpan dengan spesifikasi nama sebagai (*datetime* format YYYY- MM-DD)-(timestamp)-concat-v pada direktori applications0\com.ss.android.ugc.trill\live_data\files, format tersebut dapat diputar menggunakan perangkat lunak VLC. *Signature* video yang disimpan adalah "00 00 00 20 66 74 79 70 69 73 6F 6D 00 00 02 00 69 73 6F 6D 69 73 6F 32 61 76 63 31 6D 70 34 31" dengan arti *signature* MP4 di kode 6D 70 34.

Akun @kell_1.3 yang membuat video tentang SARA, disimpan dengan nama synthetise_2021-02-19-144205227-concat-v ekstensi "*FILE*", dapat diputar menggunakan media player VLC. Bentuk video polos tanpa memakai efek sedikitpun, video diiringi dengan musik yang berjudul "pipipi calon mantu (remix)-DJ Opus". Musik yang disediakan TikTok harus diunduh terlebih dahulu, kemudian akan tersimpan pada direktori com.ss.android.ugc.trill\live_data\files\music\download nama berkas "d7e14ff77498c0fd96eb 402c7a f71ab.mp3". Gambar 4.24 lokasi video pada direktori



Gambar 4.24 Lokasi video pada direktori dari akun kell_1.3

Akun @tanduk_2.2 yang telah dihapus hanya meninggalkan artefak video, audio dan efek yang digunakan. Video tersebut bernama "synthetise_2021-02-19-150002736-concat-v" dengan menggunakan audio 8fcb95c6d39f71d6fadff3d9ea747608.mp3. Terdapat dalam direktori \live_data\files\music\download. Efek yang digunakan dalam video ada 3 jenis pada direktori "effect" dengan Nama folder "9001edcdaaf13c76e382c102f292ee7f\

2DStickerV3_5101", "a47810f55287bbf79611fbbb16feebb1\ 2DStickerV3_5101" dan e1acc30f271518c9c5702379c6a617fe\2DStickerV3_5102.

4.8 Hasil Pengujian

Pengujian terhadap berkas XML sekitar 100 lebih item. Namun, tidak semua item di dapat informasi dari kegiatan pelaku. Berikut adalah tabel semua berkas XML yang dapat diekstrak dari telepon pintar pelaku dan telah diuji satu persatu terhadap setiap akun, sehingga dapat disimpulkan akun yang sudah dihapus tidak memiliki semua berkas XML.

Tabel 4.5 Semua Berkas XML

No	Nama Berkas	Akun		
		@karambiaaa0	@kell_1.1	@tanduk_2.2
1	ab_test_config.xml	✓	✓	
2	ai_music.xml	✓	✓	
3	app_log_encrypt_switch_count.xml	✓	✓	
4	app_notify_info.xml	✓	✓	
5	app_setting.xml	✓	✓	
6	applog_stats.xml	✓	✓	
7	apps_flyer_cache.xml	✓	✓	
8	appsflyer-data.xml	✓	✓	
9	asve_sp.xml	✓	✓	
10	AudioEffect.xml	✓	✓	
11	av_ab.xml.xml	✓	✓	
12	av_settings.xml.xml	✓	✓	
13	aweme_account_terminal_relative_sp.xml	✓	✓	
14	aweme_emoji.xml	✓	✓	
15	aweme_friends.xml	✓	✓	
16	aweme_local_video.xml	✓	✓	✓
17	aweme_user.xml	✓	✓	✓
18	aweme-app.xml	✓	✓	
19	awesome_splash.xml	✓	✓	
20	BDLocationCache.xml	✓	✓	
21	bitrate_manager_sp_rate_setting.xml	✓	✓	
22	clean_storage_pref.xml	✓	✓	
23	CLIENT_EXPERIMENT_CACHE_TAG.xml	✓	✓	
24	com.bytedance.sdk.account_setting.xml	✓	✓	
25	com.facebook.internal.preferences.APP_GATEKEEPERS.xml	✓	✓	
26	com.facebook.internal.preferences.APP_SETTINGS.xml	✓	✓	
27	com.facebook.internal.SKU_DETAILS.xml	✓	✓	
28	com.facebook.sdk.appEventPreferences.xml	✓	✓	
29	com.facebook.sdk.USER_SETTINGS.xml	✓	✓	

No	Nama Berkas	Akun		
		@karambiaaa0	@kell_1.1	@tanduk_2.2
30	com.google.android.gms.appid.xml	✓	✓	
31	com.google.android.gms.measurement.prefs.xml	✓	✓	
32	com.ss.android.ugc.trill.xml	✓	✓	
33	com.ss.android.ugc.trill_preferences.xml	✓	✓	
34	com.ss.spipe_setting.xml	✓	✓	
35	custom_channels.xml	✓	✓	
36	default_config.xml	✓	✓	
37	description.info.xml	✓	✓	
38	EditEffectConfig.xml	✓	✓	
39	extra_group.xml	✓	✓	
40	file_splash_ad_preload.xml	✓	✓	
41	gaid_sp_name.xml	✓	✓	
42	gradient_punish_warning.xml	✓	✓	
43	guide.xml	✓	✓	
44	host_monitor_config.xml	✓	✓	
45	ies_log_flag.xml	✓	✓	
46	image_opt_table.xml	✓	✓	
47	imbase_0.xml	✓	✓	
48	imbase_6896333489403724802.xml	✓	✓	
49	imbase_6930551655360414721.xml	✓	✓	
50	imbase_6930552960570000386.xml	✓	✓	
51	imbase_6930553924097590274.xml	✓	✓	✓
52	imsdk_6896333489403724802.xml	✓	✓	
53	imsdk_6930551655360414721.xml	✓	✓	
54	imsdk_6930552960570000386.xml	✓	✓	
55	imsdk_6930553924097590274.xml	✓	✓	✓
56	invite_settings.xml	✓	✓	
57	iuserstate.xml	✓	✓	
58	keva_switch_repo.xml	✓	✓	
59	key_language_sp_key.xml	✓	✓	
60	KEY_NEED_UPLOAD_LAUNCHLOG.xml	✓	✓	
61	live_sdk_core.xml	✓	✓	
62	LoginSharePreferences.xml	✓	✓	✓
63	MainTabPreferences.xml	✓	✓	
64	monitor_config.xml	✓	✓	
65	monitor_config1357p.xml	✓	✓	
66	multi_process_config.xml	✓	✓	
67	new_sp_ad_config.xml	✓	✓	
68	notice_account_related_sp.xml	✓	✓	
69	outputsettings.xml	✓	✓	
70	performance_sp.xml	✓	✓	
71	pref_name.xml	✓	✓	
72	prefs_feed_check.xml	✓	✓	

No	Nama Berkas	Akun		
		@karambiaaa0	@kell_1.1	@tanduk_2.2
73	profile.xml	✓	✓	
74	ProfilePreferences.xml	✓	✓	
75	publish.xml	✓	✓	
76	publish_sync_sp.xml	✓	✓	
77	push_multi_process_config.xml	✓	✓	
78	push_setting.xml	✓	✓	
79	rec_user.xml	✓	✓	
80	red-point-cache.xml	✓	✓	
81	search.xml	✓	✓	
82	share_setting_preference.xml	✓	✓	
83	ShortVideo.xml	✓	✓	
84	snssdk_openudid.xml	✓	✓	
85	SP_CLIENT_EXPOSURE_CACHE$$$abtest.xml	✓	✓	
86	SP_CLIENT_EXPOSURE_CACHE$$$app.xml	✓	✓	
87	sp_download_info.xml	✓	✓	
88	SP_EXPERIMENT_CACHE.xml	✓	✓	
89	SP_EXPERIMENT_EXPOSURE_CACHE.xml	✓	✓	
90	sp_show_share_guide_cache.xml	✓	✓	
91	sp_symphony.xml	✓	✓	
92	splash_ad_sp.xml	✓	✓	
93	ss_app_config.xml	✓	✓	
94	story.xml	✓	✓	
95	TeenageModeSetting.xml	✓	✓	
96	token_shared_preference.xml	✓	✓	
97	traffic_monitor_info.xml	✓	✓	
98	ttlive_sdk_shared_pref_cache.xml	✓	✓	
99	ttlive_tabs_cache.xml	✓	✓	
100	ttnet_tnc_config.xml	✓	✓	
101	ttnetCookieStore.xml	✓	✓	
102	ttplatformapi.prefs.xml	✓	✓	
103	upload_video_funnel.xml	✓	✓	
104	VerifyActionManager.xml	✓	✓	
105	version.xml	✓	✓	
106	VideoPublishManager.xml	✓	✓	
107	VideoRecord.xml	✓	✓	
108	WebViewChromiumPrefs.xml	✓	✓	
109	wschannel_multi_process_config.xml	✓	✓	

Berkas yang terpenuhi dari tiga akun adalah *aweme_user.xml.* Setiap akun akan tersimpan kegiatannya pada berkas tersebut walaupun akun telah dihapus di dalam sistem aplikasi TikTok. Setelah memeriksa semua berkas, dilakukan penyaringan keperluan

analisis agar kedepannya tidak memeriksa semua berkas yang telah diekstrak, seperti pada tabel keperluan analisis berikut.

Tabel 4.6 Keperluan Analisis

No	Nama Berkas	Keperluan Analisis		
		Sangat	Kurang	Tidak
1	ab_test_config.xml			✓
2	ai_music.xml			✓
3	app_log_encrypt_switch_count.xml			✓
4	app_notify_info.xml			✓
5	app_setting.xml			✓
6	applog_stats.xml		✓	
7	apps_flyer_cache.xml			✓
8	appsflyer-data.xml			✓
9	asve_sp.xml			✓
10	AudioEffect.xml			✓
11	av_ab.xml.xml			✓
12	av_settings.xml.xml			✓
13	aweme_account_terminal_relative_sp.xml			✓
14	aweme_emoji.xml		✓	
15	aweme_friends.xml			✓
16	aweme_local_video.xml	✓		
17	aweme_user.xml	✓		
18	aweme-app.xml		✓	
19	awesome_splash.xml			✓
20	BDLocationCache.xml			✓
21	bitrate_manager_sp_rate_setting.xml			✓
22	clean_storage_pref.xml			✓
23	CLIENT_EXPERIMENT_CACHE_TAG.xml			✓
24	com.bytedance.sdk.account_setting.xml		✓	
25	com.facebook.internal.preferences.APP_GATEKEEPERS.xml			✓
26	com.facebook.internal.preferences.APP_SETTINGS.xml			✓
27	com.facebook.internal.SKU_DETAILS.xml			✓
28	com.facebook.sdk.appEventPreferences.xml			✓
29	com.facebook.sdk.USER_SETTINGS.xml			✓
30	com.google.android.gms.appid.xml			✓
31	com.google.android.gms.measurement.prefs.xml			✓
32	com.ss.android.ugc.trill.xml			✓
33	com.ss.android.ugc.trill_preferences.xml			✓
34	com.ss.spipe_setting.xml			✓
35	custom_channels.xml	✓		
36	default_config.xml		✓	
37	description.info.xml	✓		

No	Nama Berkas	Keperluan Analisis		
		Sangat	Kurang	Tidak
38	EditEffectConfig.xml			✓
39	extra_group.xml			✓
40	file_splash_ad_preload.xml			✓
41	gaid_sp_name.xml			✓
42	gradient_punish_warning.xml			✓
43	guide.xml			✓
44	host_monitor_config.xml			✓
45	ies_log_flag.xml			✓
46	image_opt_table.xml			✓
47	imbase_0.xml			✓
48	imbase_6896333489403724802.xml		✓	
49	imbase_6930551655360414721.xml		✓	
50	imbase_6930552960570000386.xml		✓	
51	imbase_6930553924097590274.xml		✓	
52	imsdk_6896333489403724802.xml		✓	
53	imsdk_6930551655360414721.xml		✓	
54	imsdk_6930552960570000386.xml		✓	
55	imsdk_6930553924097590274.xml		✓	
56	invite_settings.xml			✓
57	iuserstate.xml			✓
58	keva_switch_repo.xml			✓
59	key_language_sp_key.xml			✓
60	KEY_NEED_UPLOAD_LAUNCHLOG.xml			✓
61	live_sdk_core.xml			✓
62	LoginSharePreferences.xml	✓		
63	MainTabPreferences.xml			✓
64	monitor_config.xml			✓
65	monitor_config1357p.xml			✓
66	multi_process_config.xml			✓
67	new_sp_ad_config.xml			✓
68	notice_account_related_sp.xml			✓
69	outputsettings.xml			✓
70	performance_sp.xml			✓
71	pref_name.xml			✓
72	prefs_feed_check.xml			✓
73	profile.xml			✓
74	ProfilePreferences.xml			✓
75	publish.xml		✓	
76	publish_sync_sp.xml			✓
77	push_multi_process_config.xml		✓	
78	push_setting.xml			✓
79	rec_user.xml			✓
80	red-point-cache.xml			✓

No	Nama Berkas	Keperluan Analisis		
		Sangat	Kurang	Tidak
81	search.xml	✓		
82	share_setting_preference.xml			✓
83	ShortVideo.xml			✓
84	snssdk_openudid.xml			✓
85	SP_CLIENT_EXPOSURE_CACHE$$$abtest.xml			✓
86	SP_CLIENT_EXPOSURE_CACHE$$$app.xml			✓
87	sp_download_info.xml			✓
88	SP_EXPERIMENT_CACHE.xml			✓
89	SP_EXPERIMENT_EXPOSURE_CACHE.xml			✓
90	sp_show_share_guide_cache.xml			✓
91	sp_symphony.xml			✓
92	splash_ad_sp.xml			✓
93	ss_app_config.xml			✓
94	story.xml			✓
95	TeenageModeSetting.xml		✓	
96	token_shared_preference.xml			✓
97	traffic_monitor_info.xml		✓	
98	ttlive_sdk_shared_pref_cache.xml			✓
99	ttlive_tabs_cache.xml			✓
100	ttnet_tnc_config.xml			✓
101	ttnetCookieStore.xml			✓
102	ttplatformapi.prefs.xml			✓
103	upload_video_funnel.xml			✓
104	VerifyActionManager.xml			✓
105	version.xml	✓		
106	VideoPublishManager.xml			✓
107	VideoRecord.xml			✓
108	WebViewChromiumPrefs.xml			✓
109	wschannel_multi_process_config.xml			✓

Pembagian klasifikasi berkas dibutuhkan dalam analisis, konteks penelitian ini dibagi menjadi 3 bagian diantaranya sangat dibutuhkan, kurang dibutuhkan dan tidak dibutuhkan. Analisis dilakukan terutama pada bagian sangat dibutuhkan seperti berkas *aweme_user, version, search* dan lain-lain.adapun kurang dibutuhkan tetap akan dianalisis untuk mendukung isi data XML dari berkas kategori sangat dibutuhkan.

Setelah melakukan analisis dapat ditentukan berkas apa saja yang diasingkan untuk dikaji lebih lanjut, berkas tersebut akan dilihat isi datanya apakah memiliki informasi penting tentang kegiatan pelaku, di dalam penelitian ini dapat diidentifikasi ada belasan berkas XML. seperti pada tabel berikut.

Tabel 4.7 Pengujian berkas XML informasi pengguna

No	Nama *File*	Akun		
		@karambiaaa	@kell_1.1	@tanduk_2.2
1	*custom_channels.xml*	✓	✓	
2	*LoginSharePreferences.xml*	✓	✓	✓
3	*aweme_user.xml*	✓	✓	
4	*aweme_local_video.xml*	✓	✓	✓
5	*search.xml*	✓	✓	
6	*Publish.xml*	✓	✓	✓
7	version.xml	✓	✓	
8	traffic_monitor_info.xml	✓	✓	
9	TeenageModeSetting.xml	✓	✓	
10	imbase_6896333489403724802.xml	✓	✓	
11	imbase_6930551655360414721.xml	✓	✓	
12	imbase_6930552960570000386.xml	✓	✓	
13	imbase_6930553924097590274.xml	✓	✓	✓
14	imsdk_6896333489403724802.xml	✓	✓	
15	imsdk_6930551655360414721.xml	✓	✓	
16	imsdk_6930552960570000386.xml	✓	✓	
17	imsdk_6930553924097590274.xml	✓	✓	✓
18	default_config.xml	✓	✓	
19	description.info.xml	✓	✓	

Sebagai catatan jika menggunakan lebih dari satu akun dalam satu perangkat, setiap kegiatan akan disimpan dalam satu berkas. Contoh pada berkas *aweme_user.xml* adalah tempat semua jejak dari setiap akun, susunannya bertingkat secara vertikal dengan urutan masing-masing akun masuk terlebih dahulu atau dengan istilah *first in first record.*

Jejak akun yang dihapus, tidak semuanya tersimpan pada berkas XML. sangat berbeda jauh dengan akun yang belum dihapus, kegiatan akun terhapus tersebut hanya terekam pada empat berkas XML diantaranya *LoginSharePreferences.xml, Publish.xml,* imbase_6930553924097590274.xml dan imsdk_6930553924097590274.xml. Informasi perangkat yang digunakan oleh pelaku dapat dilihat detailnya pada tabel berikut.

Tabel 4.8 Detail Informasi Perangkat

Detail Properties	
Manufacturer	Xiaomi
Product	Redmi 5A
HW Revision	OPM1.171019.026

Detail Properties	
Platform	Android
SW Revision	8.1.0 (27)
Android ID	869f3eef23d86f52
Serial Number	89149b4a7ce5
Device Time	2021-02-22 19:02:17 (UTC+7)
Manual Time	No
Time Zone	Asia/Jakarta
Manual Time Zone	No
Device Storage Encrypted	Yes
IMEI	868698036296806
IMEI 2	868698036296814
LACCID	LAC: 3612, CID: 24215440
Rooted	Yes
SIM Card	No
Total Storage	9.7 GB
Used Storage	4.9 GB
Sumber	imei.info

Detail informasi dari telepon pintar dapat dilihat dari website imei.info dengan memasukkan nomor imei perangkat, pada perangkat ini imeinya dapat dilihat bagian belakang di dalam. Sebagian telepon seluler mencantumkan nomor imei di luar bagian belakang, tetapi dapat juga menggunakan nomor panggilan *#06#. Aplikasi TikTok yang digunakan dapat dilihat pada tabel berikut.

Tabel 4.9 Detail aplikasi TikTok yang digunakan

Detail Aplikasi	
Label	TikTok
Package	com.ss.android.ugc.trill
Version	16.6.4
Application Type	User Application
Sideloaded Application	Yes
Installed by	com.google.android.packageinstaller
Application Size	90.8 MB
Cache Size	0 B
APK File Extracted	Yes
APK Verification Successful	Yes
APK Verification Scheme	2
Best Certificate Found	Cert 00a584e375b5573c89e1f06f5cf60d0d65ddb632, valid from 2011-12-31T08:35:54Z to 2039-05-18T08:35:54Z, Subject: C=CN, ST=Beijing, L=Beijing, O=ByteDance, OU=ByteDance, CN=Micro Cao, Issuer: C=CN, ST=Beijing, L=Beijing, O=ByteDance, OU=ByteDance, CN=Micro Cao
Lokasi berkas XML	phone_files\phone\applications0\com.ss.android.ugc.trill\description.info.xml

Pada aplikasi TikTok segala informasinya dapat dilihat pada lokasi berkas phone_files\phone\applications0\com.ss.android.ugc.trill\description.info.xml. Informasi yang diberikan sangat banyak seperti lokasi paket, versi, tipe aplikasi, ukuran dan lain-lain. Akun yang digunakan adalah tiga buah dalam satu aplikasi TikTok, setiap akun memiliki skenario masing-masing. Akun Karambiaaa adalah akun asli, Akun Kell_1.3 adalah yang mengirim pesan dan akun Tanduk_2.2 yang dihapus. tabel berikut adalah detail untuk akun Karambiaaa.

Tabel 4.10 Akun Karambiaaa0

Detail Akun	
Nickname	Karambia aa
Register at	2020-11-18 12:51:22 (UTC+7)
User ID	6896333489403724802
Profile Picture	https://p16-sign-sg.tiktokcdn.com/aweme/1080x1080/tiktok-obj/ 1683676134080514.webp?x-expires=1613808000&x- signature=c0yl3kaEu8mSwtYB9GiEEcRJmLA%3D
Lokasi Berkas XML	phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\Aweme_user.xml

Segala informasi pada akun di aplikasi TikTok dapat diambil dari lokasi berkas XML phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\Aweme_user.xml. Informasi yang diberikan mulai dari *nickname, register at, user id* juga *profile picture.* Tabel berikut adalah tentang akun Kell_1.3.

Tabel 4.11 Akun kell_1.3

Detail Akun	
Nickname	Kell_1.3
Register at	2021-02-18 19:08:26 (UTC+7)
User ID	6930551655360414721
Profile Picture	https://p16-sign-sg.tiktokcdn.com/musically-maliva-obj/ 1594805258216454~c5_1080x1080.webp?x-expires=1613808000&x- signature=re3HHNF98wm%2FUaZHqr9hxiZmlIQ%3D
Lokasi Berkas XML	phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\Aweme_user.xml

Akun Kell_1.3 informasinya dapat juga dilihat pada lokasi berkas phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\Aweme_u

ser.xml. informasi item yang diberikan tidak berbeda dengan akun Karambiaaa sebelumnya. tabel berikut informasi akun Tanduk_2.2.

Tabel 4.12 Tanduk_2.2

Detail Akun	
Nickname	tanduk_2.2
User ID	6930552960570000386
Lokasi Berkas XML	phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\Aweme_user.xml

Berbeda dengan akun-akun sebelumnya, akun yang telah dihapus tidak banyak informasi yang didapat hanya sebagian kecil saja artefak yang ditinggalkan, seperti *user id.* Tabel berikut adalah detail pencarian.

Tabel 4.13 Detail Pencarian

Detail Pencarian	
Nickname	Kell_1.3
Register at	2021-02-18 19:08:26 (UTC+7)
User ID	6930551655360414721
Kata Kunci Pencarian	muhammadromi_0.1 khoax karambiaaa0 tanduk_2.2 jack_0.4 sara agama
Lokasi Berkas XML	phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\search.xml

Sesuai skenario akun yang melakukan pencarian dalam aplikasi TikTok adalah Kell_1.3. Kata kunci yang dipakai dalam pencarian semua tersimpan pada direktori phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\search.xml. Tabel berikut tentang percakapan antar akun.

Tabel 4.14 Tabel Percakapan

Detail Percakapan	
Terakhir Update	2021-02-19 15:11:03 (UTC+7)
Jumlah Tidak Terbaca	0
Jumlah Member	2
Peserta	6896334472335590402 (@muhammadromi_0.1), 6930551655360414721 (@kell_1.3)
Dari	6930551655360414721
Ke	6896334472335590402
Data	{"type":0,"isDefault":false,"text":"jelek Lo mirip banget aa monyet \ntolol bodoh eek lo","is_card":false,"mSendStartTime":1613722263921,"msgHint":"","aweType":700}
Percakapan	jelek Lo mirip banget aa monyet tolol bodoh eek lo
Lokasi Berkas DB	phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\databases\6930551655360414721_im.db

Percakapan yang dilakukan antar akun wajib dengan syarat saling mengikuti, penelitian ini menemukan bahwa akun yang hanya mengikuti tetapi tidak diikuti balik maka tidak bisa melakukan pertukaran pesan. Informasi percakapan yang dilakukan tersimpan

dalam bentuk ekstensi DB yang dapat dibuka dengan aplikasi DBbrowser terletak pada folder phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\databases\6930551655360414721_im.db. Data percakapan dapat dikonversikan ke visual XML seperti berikut {"type":0,"isDefault":false,"text":"jelek Lo mirip banget aa monyet \ntolol bodoh eek lo","is_card":false,"mSendStartTime":1613722263921,"msgHint":"","aweType":700}. Tabel berikut informasi video Tanduk_2.2.

Tabel 4.15 Tabel Video Tanduk_2.2

Detail Video	
Nama Bekras	synthetise_2021-02-19-144205227-concat-v
Ekstensi	FILE
Nama Musik	d7e14ff77498c0fd96eb 402c7a f71ab
Ekstensi	Mp3
Lokasi Video	phone\applications0\com.ss.android.ugc.trill\live_data\files
Lokasi Mp3	phone\applications0\com.ss.android.ugc.trill\live_data\files\music\download
Lokasi Berkas XML	phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\aweme_local_video.xml
ID Akun	6930553924097590274

Berbeda dengan informasi akun lain. Artefak yang ditemukan untuk akun yang telah dihapus pada bagian video sangat lengkap. Setiap video yang dibuat pada aplikasi TikTok akan tersimpan pada phone\applications0\com.ss.android.ugc.trill\live_data\files. video tersebut memiliki ekstensi *FILE,* Nama berkasnya synthetise_2021-02-19-144205227-concat-v, aplikasi pemutar pada OS Windows dapat menggunakan Media Player Classic. Musik yang digunakan juga dapat ditemukan pada folder phone\applications0\com.ss.android.ugc.trill\live_data\files\music\download. Tabel berikut informasi video akun Kell_1.3.

Tabel 4.16 Tabel video akun Kell_1.3

Detail Video	
Nama Bekas	synthetise_2021-02-19-150002736-concat-v
Ekstensi	FILE
Nama Musik	8fcb95c6d39f71d6fadff3d9ea747608
Ekstensi	Mp3
Lokasi Video	phone\applications0\com.ss.android.ugc.trill\live_data\files
Lokasi Mp3	phone\applications0\com.ss.android.ugc.trill\live_data\files\music\download
Lokasi Berkas XML	phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\aweme_local_video.xml
ID Akun	6930551655360414721

Lokasi berkas video dapat ditelusuri melalui XML yang terdapat pada phone_files\phone\applications0\com.ss.android.ugc.trill\live_data\shared_prefs\aweme_local_video.xml. Posisi artefak yang ditinggal tidak jauh berbeda dari akun Tanduk_2.2 yaitu di folder phone\applications0\com.ss.android.ugc.trill\live_data\files. Semua jenis informasinya juga sama dengan akun lain contohnya ekstensi, nama berkas yang mengikuti tanggal hari unggahan tersebut.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan dapat ditarik kesimpulan beberapa karakteristik dan pemetaan terhadap artefak dari aplikasi TikTok:

1. Lebih dari 100 item artefak yang dapat diekstrak. Namun, tidak semua berkas XML terdapat catatan kegiatan semua akun, untuk akun yang belum dihapus akan terdapat penuh informasinya. Sangat berbeda dengan akun yang telah dihapus, informasi yang tercatat hanya berupa beberapa berkas XML, kegiatan-kegiatan tersebut adalah masuk aplikasi dan catatan unggah video.
2. Karakter data yang disimpan, berupa *folder* phone file digunakan hampir seutuhnya artefak kegiatan di aplikasi TikTok terutama di berkas ugc trill. Tetapi, beberapa berkas XML berada di luarnya seperti cell info adalah sumber informasi dari sinyal yang digunakan saat tersambung internet.
3. Semua gambar memiliki jumlah sekitar 200 item lebih, karakter dari gambar secara garis besar ada 4 bagian pertama Nama seperti img_7216, img_7217 dan seterusnya, selain itu menggunakan format tahun bulan dan tanggal kemudian akhiran nama "cover" pada sebagian gambar seperti ,gambar-gambar yang ada yaitu hasil dari belhan video menjadi gambar dan ekstensi dalam kompres potongan gambar menggunakan png.
4. Saat masuk aplikasi TikTok akan secara vertikal tersimpan artefaknya, berkas XML yang cukup lengkap informasinya dari 3 akun adalah *awemeuser*.xml seperti tempat pencatatan alamat masuk, *username,* metode masuk, terakhir diakses dan lain-lain. Dapat disimpulkan informasi terbanyak ada pada berkas tersebut.
5. Karakter dari akun yang dihapus begitu unik karena hanya memiliki beberapa artefak untuk dianalisis seperti pada tabel Semua Berkas XML. Hasil analisis informasi terbanyak terdapat pada aweme_local_video.xml dan LoginSharePreferences.xml. aweme_local_video.xml adalah tempat penyimpanan jejak kegiatan unggah video, jadi letak direktori dari berkas video dapat dilihat pada file XML tersebut. LoginSharePreferences.xml adalah informasi login akun yang telah dihapus.
6. Penelitian sebelumnya ada tiga tanda dalam berkas media seperti tanda "v" untuk video, "a" untuk audio dan "mix-concat-a" campuran antara video dan audio. Tetapi,

hal tersabut tidak berlaku lagi dalam artefak yang dianalisis pada penelitian ini, hasilnya video akan tersimpan dengan format nama “concat-v” saja.

5.2 Saran

Saran untuk penelitian selanjutnya adalah:

1. Penelitian ini berfokus pada berkas XML untuk melihat seperti apa karakter artefak yang apabila menggunakan lebih dari satu akun di satu perangkat. Sebagai masukan untuk kajian selanjutnya melakukan penelitian terhadap artefak perangkat iphone atau berkas Plist. Bahkan akan lebih menarik menggunakan tiga akun dalam aplikasi tiktok cloning.
2. Melakukan pengujian terhadap kasus nyata di dunia forensic digital, agar metode pada penelitian ini dapat diukur keakuratan peta dan karakteristik dari bukti digital berdasarkan artefak yang ditinggalkan.

Daftar Pustaka

Al-Dhaqm, A., Razak, S. A., Ikuesan, R. A., Kebande, V. R., & Siddique, K. (2017). A Review of Mobile Forensic Investigation Process Models. *IEEE Access*, *8*, 173359–173375. https://doi.org/10.1109/access.2020.3014615

Ali, A., & Fazeel. (2016). Forensic examination of social networking applications on smartphones. *Proceedings - 2015 Conference on Information Assurance and Cyber Security, CIACS 2015*, 36–43. https://doi.org/10.1109/CIACS.2015.7395564

Anglano, C. (2014). Forensic analysis of whats app messenger on Android smartphones. *Digital Investigation*, *11*(3), 201–213. https://doi.org/10.1016/j.diin.2014.04.003

Anglano, C., Canonico, M., & Guazzone, M. (2017). Forensic analysis of Telegram Messenger on Android smartphones. *Digital Investigation*, *23*(October), 31–49. https://doi.org/10.1016/j.diin.2017.09.002

Cedillo, P., Camacho, J., Campos, K., & Bermeo, A. (2019). A forensics activity logger to extract user activity from mobile devices. *2019 6th International Conference on EDemocracy and EGovernment, ICEDEG 2019*, 286–290. https://doi.org/10.1109/ICEDEG.2019.8734298

Domingues, P., Nogueira, R., Francisco, J. C., & Frade, M. (2020). Post-mortem digital forensic artifacts of TikTok Android App. *ACM International Conference Proceeding Series*, *August*. https://doi.org/10.1145/3407023.3409203

Döring, H., & Wei, Y. (2012). A study on the performance of a gyromonotron. *International Journal of Infrared and Millimeter Waves*, *2*(3), 437–452. https://doi.org/10.1007/BF01007412

Garfinkel, S. (2012). Digital forensics XML and the DFXML toolset. *Digital Investigation*, *8*(3–4), 161–174. https://doi.org/10.1016/j.diin.2011.11.002

Hoang Khoa, N., The Duy, P., Do Hoang, H., Thi Thu Hien, D., & Pham, V. H. (2020). Forensic analysis of TikTok application to seek digital artifacts on Android smartphone. *Proceedings - 2020 RIVF International Conference on Computing and Communication Technologies, RIVF 2020*. https://doi.org/10.1109/RIVF48685.2020.9140739

Laurenson, T., MacDonell, S., & Wolfe, H. (2015). Towards a standardised strategy to collect and distribute application software artifacts. *Australian Digital Forensics Conference, ADF 2015*, *2015*, 54–61. https://doi.org/10.4225/75/57b3f5cffb889

Musleh, I., Zain, S., Nawahdah, M., & Salleh, N. (2018). Automatic generation of android SQLite database components. *Frontiers in Artificial Intelligence and Applications*, *303*(September), 3–16. https://doi.org/10.3233/978-1-61499-900-3-3

Nemetz, S., Schmitt, S., & Freiling, F. (2018). A standardized corpus for SQLite database forensics. *DFRWS 2018 EU - Proceedings of the 5th Annual DFRWS Europe*, *24*, S121–S130. https://doi.org/10.1016/j.diin.2018.01.015

Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K. K. R. (2016). Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. *Australian Journal of Forensic Sciences*, *48*(4), 469–488. https://doi.org/10.1080/00450618.2015.1066854

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of android social-messaging applications. *Proceedings of the Digital Forensic Research Conference, DFRWS 2015 USA*, *14*, S77–S84. https://doi.org/10.1016/j.diin.2015.05.009

Wang, Y. H., Gu, T. J., & Wang, S. Y. (2019). Causes and Characteristics of Short Video Platform Internet Community Taking the TikTok Short Video Application as an Example. *2019 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW 2019*, 4–5. https://doi.org/10.1109/ICCE-TW46550.2019.8992021

Weimann, G., & Masri, N. (2020). Research Note: Spreading Hate on TikTok. *Studies in Conflict and Terrorism*, *0*(0), 1–14. https://doi.org/10.1080/1057610X.2020.1780027

Yu, J. X. (2019). Research on TikTok APP Based on User-Centric Theory. *Applied Science and Innovative Research*, *3*(1), 28. https://doi.org/10.22158/asir.v3n1p28